Dialog®

Refs Search within these results:

L1 play and digital and content and license and rights and encryption and streaming and authentication and subsequent

Enter Search Terms

Search

Perform New Search
Choosing this option will erase previous sets.

Core RT1 (7)
Core RT2 (7)

Records: 1 to 7 of 7

Display Selected ☑ Highlight Selected Clear All (0 of 100 selected)

Sort by: Date (Newest to Oldest

Check All

☐ Accelerating consumers' NAS adoptions: assessing your product options.

Date: June 25 , 2009

3/6,K/1 (Item 1 from file: 148)
0025432884 **Supplier Number:** 202192257 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Accelerating consumers' NAS adoptions: assessing your product options.

June 25 , 2009
Word Count: 4590 **Line Count:** 00385

...common Internet connection but also intercommunicate.
All of these trends suggest the allure of a consolidated nexus in consumers' residences for both professional and personal **content** that multiple LAN clients could simultaneously access. Ideally, this centralized storage would implement a RAID (redundant array of independent disks), which would protect the NAS...

...mode it's in at the time. And the need to provide the NAS with both the

WLAN (wireless-LAN) SSID (service-set-identifier) and **encryption** -key information before it can make the Wi-Fi connection is a challenging setup requirement for a headless-system design. Finally, you need to decide ...

...counterparts will be advocating that your customers should use the NAS as a single-point-of-storage contact for all of their precious--often irreplaceable--**digital** data: music libraries, photographs, videos, financial records, and the like. Unless you use a RAID 1, RAID 5, or other mirrored-drive arrangement, such as...

...regarding how the NAS market may evolve in the future. Today's NAS suppliers include traditional hard-disk-drive companies, such as Seagate and Western **Digital**; traditional network-equipment vendors, such as Cisco's Linksys division, D-Link, and Netgear; and start-ups, such as Data Robotics. Hard-disk-drive companies...
...your users will likely want to be able to carve up the available capacity into more than one shared-storage resource, with per-share access **rights**, such as disabled, read-only, or read/write, that customers will define on a per-user and -group basis. They'll access the networked storage...

...AFP (Apple-filing protocol), NFS (network-file system), and SMB/CIFS (server-message block/common Internet-file system). They'll also want both configuration and **subsequent** access to work in a way that doesn't force them to comprehend and grapple with the underlying complexity.
LAN-client backup, another commonly requested...

...consider the laundry list of other NAS capabilities that your potential customers might value and, therefore, pay extra for. These features include on-the-fly **encryption** during storage and **subsequent** decryption during read-back of information archived on the NAS, along with USB (Universal Serial Bus) ports for printer serving, augmented storage capacity, and networked access to scanners and other USB peripherals. Your customers might also want automatic network discovery through protocols such as UPnP (universal plug and **play**) and Apple's Bonjour--that is, Zeroconf. Media **streaming** is also on the list. Protocols such as UPnP AV (audio/video) and DLNA (**Digital** Living Network Alliance) enable this feature both across the LAN and over a WAN (wide-area-network) connection. Firewall-surmounting technologies, such as UPnP and...

...safeguards that ISPs (Internet-service providers) now put in place. These potential roadblocks include nonstandard SMTP (simple-mail-transfer-protocol) ports, user-name and password **authentication** at the SMTP server, and SSL (secure-sockets-layer) capabilities.
Keep in mind, too, that you must support no-brainer updates to the NAS BIOS...

...optimized IC variants. In addition, consider not only architecture-tailored software from your company but also that of third-party software you might want to **license**, along with additional utilities that your customers may want to install after the purchase. For example, many enthusiasts have developed freely downloadable add-ons for...

...Semiconductor's R3210 CPU, implementing the i486 microprocessor-instruction set. However, the NAS was so performance-strapped that it couldn't support either SMTP-server **authentication** or SSL cognizance for e-mail alerts; it also could not use its USB port to implement a print server. Similarly, the company initially shipped...

...a Casetronic Travla C137 enclosure (Figure A). I customized the C137 to hold dual 3.5-in. hard-disk drives from both Seagate and Western **Digital** for mirrored storage. Because many of the NAS systems on the earlier list use modified Linux distributions, I focused this evaluation on Windows Home Server...

...the foundation of your next NAS design, I'd encourage you to focus some tangible effort in polishing these areas and, per the open-source **license**, to return your results to the organization so that it can incorporate your improvements.

One other minor frustration involved the EPIA SN BIOS (basic input ...

...horsepower in some configurations (Reference B). Also, if you're doing PVR (personal-video-recorder) applications, such as video encoding before archiving or transcoding before **streaming**, you might want to consider using the three-way-superscalar, out-of-order architecture that Via includes in its Nano CPU and implements in its...

...seagate.com
www.maxtor.com
Sony
www.sony.com
Toshiba
www.toshiba.com
Tritton Technologies
www.trittontechnologies.com
Via Technologies
www.via.com.tw
Western **Digital**
www.wdc.com
Ximeta
www.ximeta.com

You can reach Senior Technical Editor Brian Dipert at 1-916-760-0159, bdipert@edn.com , and www...

View: HTML | PDF | Word

☐ Indexing and retrieval of multimedia metadata on a secure DHT.(distributed hash table)(Report)

Date: March , 2009

3/6,K/2 (Item 2 from file: 275)
03585629 **Supplier Number:** 203134703 **(Use Format 7 Or 9 For** FULL TEXT)
Indexing and retrieval of multimedia metadata on a secure DHT.(distributed hash table)(Report)

March , 2009
Word Count: 12081 **Line Count:** 01004

Text:

This paper proposes a decentralized, distributed and secure communication infrastructure for indexing and retrieving multimedia contents with associated **digital rights**. The lack of structured metadata describing the enormous amount of multimedia contents distributed on the the web leads to simple search mechanisms that usually are...

...and MPEG-21 multimedia metadata. Moreover, security aspects limit the development of general purpose real applications using a peer-to peer routing infrastructure for sharing **digital** items with an associated **license**. Accordingly, we propose a framework made up of a secure Distributed Hash Table layer based on Kademlia, including an identity based scheme and a secure...

Keywords: multimedia metadata, **digital rights**, secure distributed hash table, peer-to-peer

Povzetek: Predstavljen je sistem za ucinkovito indeksiranje in doseganje digitalnih vsebin.

1 Introduction

Nowadays the growing of **digital** items exchanged on the web increases the need of their accurate description. We can define metadata as the description of the data. Even if it is possible to share multimedia items, it is very difficult or impossible to search them without appropriate description provided by **content** metadata. Usually people making use of web-sharing systems do not provide detailed metadata information, which in most cases is only limited to the ...unstructured information. Using metadata it is possible to structure the information and thus, on one side, to enhance and enrich the information related to a **content** and, on the other, to search and retrieve **digital** items. It is clear that more detailed are the metadata, more complex is the structure which they are inserted on.

Moreover, in order to reach a common understanding of metadata, it is important to adopt standards. The adoption of MPEG-7 (1) for describing metadata related to the **digital** items and of MPEG- 21 (2) for describing metadata related to a governed **content** (i.e., with an associated **license**), as proposed in this paper, is a common approach used by an increasing number of scientific communities. The use of the standards mentioned above can improve the expressiveness of the query language for the multimedia items and can make governable the **content** distribution.

The enormous amount of media available on the web promotes the adoption of completely decentralized infrastructures, such as peer-to-peer (P2P) **content** sharing systems, that minimize the impact of a single point of failure fostering scalability, reliability and efficiency. Unfortunately, such approaches introduce a large spectrum of security flaws that limit the adoption in a real scenario. In fact, if it is true that **digital** contents are growing up very lastly especially in such distributed environments, it must be noticed that such systems usually offer poor functionalities for indexing and...

...affects these systems: the lack of a central entity offering a complete representation of complex information (i.e., the set of the metadata characterizing the **digital** items) results in a poorly expressive query language (e.g., parsing of the query string and pattern matching). Moreover most of these topologies are not providing any kind of **content** government and in the worst case they are not taking into account any **digital rights** associated to the exchanged resources.

We propose a decentralized, distributed and secure communication infrastructure for the indexing and the retrieval of governed as well as... ...contents. Our approach, based on Distributed Hash Tables, allows complex queries to the system by means of complex multimedia metadata indexing. Moreover, the sharing of **digital** items on the basis of the associated **license** (either free or not), enables ...of our work are summarized in the following:

--a decentralized scheme to index and retrieve structured metadata related to multimedia contents,

--a policy to manage **digital rights** expressed by MPEG-21 **Rights** Expression Language (REL) (3) profiles that enables the governed sharing of **digital** items along with the protection of the intellectual property, a secure structured overlay network that assures the basic security functionalities providing an effective defense against...presented.

For metadata representation we adopted the MPEG-7 (1) and MPEG-21 (2) standards, which are outlined in Section 2.3. Concerning the governed **content** management, we adopted the solutions developed by the **Digital** Media Project (DMP) (4). Accordingly, Section 2.3.1

describes the overall architecture of Chillout (5), the reference software implementation of the ISO/IEC 23000-5 (Media **Streaming** Application Format) standard.

2.1 Distributed Hash Tables

Distributed Hash Tables (DHTs) (6, 7, 8) are a class of distributed algorithms that provides the same...the target identifier are initiated, intercepting thus most of the lookup requests and answering with fake contents or not replying at all, effectively hiding the **content**.

Since typically there exists no verifiable link between the participating entity (human user or machine) and its identity (the nodeId), it is possible for any few machines, centralizing unsafely many keys' responsibilities and **content** replicas. The Sybil entities are usually exploited to increase the effectiveness of other attacks (e.g., Eclipse, DDoS) without needing huge computational resources or without...

...other colluding entities.

An index poisoning based attack (10) consists in inserting corrupted contents among the storages of a group of index nodes. A corrupted **content** might be something not related to the key for which it was stored, or even a fake information, like a reference to the wrong source. An attacker can make a bogus **content** highly visible by flooding fictitious records under 'strategic' indexes (e.g., among nodes responsible for "hot" keys), flushing legitimately stored **content**. In file-sharing applications, the most similar attack is the **content** pollution, that inserts on the DHT fake meta-data (i.e., meta-data that should be correct but that point to corrupted resources).

A distributed an index poisoning attack. In file-sharing systems, the attacker can insert meta-data related to a very popular **content**, pointing to the target IP address as a source of such a file: the victim will be overflowed by connection requests until the 'polluted' **content** will be kept in index nodes' storage.

Concluding this overview on the attacks, it is worth notice that some studies (12) show that in the...completing the puzzles of all nodes in the chain are provided a cryptographic proof of the examined identity.

A tool which could effectively combat the **content** pollution and the index poisoning attacks is the use of credentials, bound to the **content**, provided by the owner of the **content** during the insertion phase: if the **content** is bound to the identity of an owner, when a fake resource is found, it is possible to trace back to **content** creator. If the application implements a reputation system, it could be possible to penalize or even to ban a malicious node.

Credentials and reputation systems can also be used against DDoS: as it would be too costly to oblige replica nodes to verify the authenticity of each inserted **content**, it is necessary to adopt a reputation system so that peers who have made incorrect insertions are recognized as soon as possible and banned from...groups nd match them with appropriate cryptographic techniques and protocols is presented in (26).

2.3 Multimedia Metadata Representation

MPEG-7 (1), formally named Multimedia **Content** Description Interface, provides a rich set of standardized tools to describe multimedia contents. It mainly focuses on description of the **digital** items, without considering how and where this information is used. In particular, the MPEG-7 descriptions of **content** may include (1) information describing the creation and production processes of the **content** (director, title, short feature movie), (2) information related to the usage of the **content** (copyright pointers, usage history, broadcast schedule), (3) information of the storage features, (4) on spatial, temporal or spatio-temporal components or about low level features (colors, textures, sound timbres, melody description) and many others.

MPEG-7 standard has been included in several metadata language, such as ODRL (Open **Digital Rights** Language) (3) and has

been coupled with other important TV ontologies (e.g., TVAnytime RMPI (27)). Concerning **digital rights**, MPEG-7 provides a standard XML schema and the metadata to define conditions for accessing the **content** (including links to a registry containing intellectual property **rights** data and price) and additional information about the **content** (copyright pointers, usage history, broadcast schedule). An MPEG-7 Query Format reached the Final Committee Draft, during the MPEG meeting on October 2007. Moreover several framework to be used by all the players in the delivery and consumption value chain. This framework will provide an open market to **content** creators, producers, distributors and service providers. The goal of MPEG-21 is the definition of a standard technology needed to support users in order to exchange, access, consume, trade and otherwise manipulate **digital** items in an efficient, transparent and interoperable way. In particular, part 5 of MPEG-21 defines a **Rights** Expression Language (REL) to be used in the description of customized **rights** applied to any **digital** item, since it is seen as a machine-readable language that can declare **rights** and conditions defined in the **Rights** Data Dictionary (also standardized by MPEG-21). **Rights** metadata are expressed by means of MPEG-21 REL, which describes the **license** associated to a specific resource, along with several available **rights** (**play**, copy, modify, print, etc.). According to the schema shown in Figure 1 (29) we can imagine the **license** as made up of an issuer (with multiplicity 0 or 1), an undefined number of grants (multiplicity 0 or more), and a principal (multiplicity 0 or 1). The issuer is the owner of the **rights** associated to a given **content** (eventually coincident with the creator or distributor of the resource) and can assign a given right (e.g., the authorization to copy or modify the **content**) to the principal. For example, in the wide commonly used CreativeCommons (30) licenses the principal is not specified since this kind of **license** is intended for everyone.

2.3.1 Chillout

Chillout (5) is the reference software of the **Digital** Media Project (DMP) (4). DMP is a no profit organization that has recently approved a version 3.0 of its specification, called Interoperable DRM Platform (IDP-3.0). Chillout is also the reference implementation of ISO/IEC 23000-5 Media **Streaming** Application Format (31), addressing the distribution of governed **content** over **streaming** channels. The most important technologies adopted by Chillout are: (a) a data structure capable of hosting different data types accompanying a resource (e.g., audio, video, image, text, etc.), (b) a **content** identification system, (c) a set of technologies for **content** protection, (d) the **Rights** Expression Language, (e) a file format for storing **digital** items and resources and (f) a technology to transmit **digital** items in **streaming** mode.

Two file formats for managing **digital** contents are used as depicted in Figure 2: DCI (DMP **Content** Information) and DCF (the DMP **Content** File) (32). The DCI is a standard XML-based format which is intended mainly to express the **license** metadata and is compliant with two MPEG-21 REL profiles: the Open Access **Content** (OAC) profile (33), for expressing equivalent CreativeCommons licenses, and the Dissemination And Capture (DAC) profile (34), mapping the TV Anytime RMPI (35) licenses, used in the broadcasting domain. The specification of the DCI allows also to include the MPEG-7 representation for the **content**. The DCF file has been conceived as a container of the DCI and the ...system that is able to share governed contents on P2P networks, where share here means the possibility to publish, index, search, retrieve and consume a **digital** item and governed refers to the fact that each **digital** **content** distributed on such system is governed according to its associated **license**. It is worthwhile pointing out that a DRM system could use the proposed solution as the underlying software to manage

(create, index, retrieve) governed contents, demanding to an other application software placed on top of it to manage or not the associated **digital rights**. This solution allows also the integration of the proposed prototype with proprietary DRM solutions, where the **content** representation is based on MPEG standards. Moreover, despite the common feeling about P2P networks in relationship with abuse or violation of **digital rights** and intellectual property **rights** in general, mainly due to the sharing of copyrighted or otherwise licensed **content**, the software solution proposed in this paper proofs that it is possible to have **content** government on these popular networks and is also possible to make them secure.

(FIGURE 2 OMITTED)

We make use of the MPEG-7 standard for expressing the metadata related to the **digital content** itself, describing the user metadata (e.g., title or author) as well as the metadata describing the **content** as visual descriptors (e.g., ScalableColor or HedgeHistogram). We have adopted the MPEG-21 standard for expressing licenses because MPEG-21 REL provides several profiles for specific environments and purposes (broadcasting, mobile applications...), which guarantee high interoperability with other **rights** languages and therefore it is able to express most of the possible licenses. As described in Section 2.3.1 Chillout can manage governed **content** using MPEG-7 and MPEG-21 representation, which is contained into a DCI structure, specified by ISO/IEC 23000-5. Hence the proposed solution is...approach is made up of three logic layers:

--User Interaction Layer, where the several user software components communicate with the application layer providing and consuming **digital** contents.

--Application Layer, which is in charge for extracting the information to be indexed and for communicating with the DHT layer in order to index components depicted in Figure 3, a user device can **play** different roles:

--**Content** Creator, which is the component responsible for the creation of governed **content** (in DCF format), making use of user resources and the associated licenses (expressed in the DCI file).

--**Content** Provider, which is the component responsible for providing governed contents that can be created by the same user as well as by others.

--Player (End...

...the component that can consume the resources according to the associated licenses. When the user asks the system to consume a resource, it recognizes which **rights** are guaranteed to the current user (e.g., copy, **play**, modify, distribute) and can enforce them.

The Application Layer is made up of three main components: Retrieving, Indexing and Exchanging, as shown in Figure 3...layer and (d) inserting the relative mappings in the DHT.

A user can search for resource related metadata (e.g., the title in MPEG-7), **license** related metadata (e.g., the issuer in MPEG-21 REL) or a combination of the two. A detailed description of the Retrieving and Indexing components...Figure 3 using UML 2.0 (36) conventions), one for exchanging metadata information that are basically DCI documents and the other for exchanging the real **digital content**, for example as byte array. This communication is asynchronous and completely separated. The user can make use of the metadata exchanging component looking for several...there is a discrepancy between metadata representation and the way in which information are stored in a DHT-based infrastructure. In the first case, the **content** is described by a structured XML-based formalism, e.g., MPEG-7 and MPEG-21 ...proposed an iterative indexing and retrieving scheme (37) that is similar to the hierarchical indexing scheme described in (38).

Let's consider a genetic audiovisual **content** R that is associated with a set of metadata. Such metadata are extracted during the

indexing phase from the MPEG-7 and/or MPEG-21 and **digital rights**. Therefore, it is evident that to index the complete metadata knowledge could represent a very expensive computational and spatial cost. To lighten the load of...it calculates (id.sub.mi) and, by means of a lookup({id.sub.mi}), it retrieves the identifier of the corresponding resource. At last, a **subsequent** lookup is able to get {directly or indirectly} the requested resource.

A key aspect of our approach is the ability to index and retrieve audiovisual items with associated **digital rights**. We can divide contents between governed and ungoverned. Ungoverned items do not have licenses associated and the keywords to be indexed are just MPEG-7 elements. Governed items have a **license** and we have defined the following structure to be indexed: for each right described in the **license** we index three MPEG-21 REL tags: issuer, right, principal {see Section 2.3}. Although typical licenses contain one or more grants, we assume in the following a single issuer and a single principal for each right and for every grant expressed in the **license** we index the bundle of issuer, right and principal linking the associated **content**. Hence, the DHT contains the indexes of the general purpose metadata and in addition, for governed resources, the bundle of grants linking the **digital** item.

{FIGURE 3 OMITTED}

Figure 4: Example of a MPEG-7 description for a MP3 audio file.

```
<?xml version="1.0" encoding="UTF-8"?>
<Mpeg7...ID3genreCS:vi:80-><Name>
            Acoustic Rock</Name></Genre>
        </Classification>
      </CreationInformation>
    </Description>
</Mpeg7>
```

Let's consider again the resource R with an associated MPEG-21 REL **license** as shown in Figure 5. We extract the following metadata elements:

(m.sub.issuer) = (issuer...**play**). The principal is not defined since the item is governed by a Creative Commons **License** . Afterwards, a key is calculated for the metadata, i.e., (id.sub.issuer), (id.sub.right) and (id.sub.princip) respectively, and the mappings <(id ...m.sub.princip)), (id.sub.R)>

In this scenario, a user could search for "all the **digital** items issued by someone", or could submit composite queries like " ... above.

5 Secure DHT Layer based on Kademlia

As previously underlined, one of the main concern that limits a broad adoption of a DHT-based **content** sharing platform is the security aspect. In this Section we will describe a communication protocol and an identity management scheme that provide a secure layer...no control is performed by replica nodes over the information stored in the DHT thus allowing the index poisoning and derivative attacks. There is no **authentication** protocol between nodes. Nevertheless, k-buckets provide resistance to certain DoS and index pollution attacks; in fact, one cannot flush nodes routing state by flooding...message m signed with key k

```
H(o)                    :  hash code of the object o
(Auth:id.sub.A)         :  node A's authenticated id
(Auth sub.AB)           :  authentication
by A for B
ts, TTL                 :  timestamp, time to live
astrings
```

Figure 5: Example of a MPEG-21 REL **license** for the audio file described in Figure 4.

```
<?xml version="1.0" encoding="UTF-8"?>
```

<license xmlns="urn:mpeg:mpeg21:2003:01-REL-R-NS,
xmlns:mx="urn:mpeg:mpeg21:2003:01-REL-MX-NS,, xmlns:m3x="urn:mpeg:
mpeg21:2006:01-REL-M3X-NS">
<grant>
<mx:play/>
<digitalResource licensePartId="jj-2005-onon-track-01">
<nonSecureIndirect URI="urn:newspaper:
news:2005 ...copyrightString> Written by Jack Johnson,
2005</m3x:copyrightString>
</m3x:copyrightNotice>
</grant>
<issuer>
<keyHolder>
<info>
<dsig:KeyName>Jack Johnson's
key</dsig:KeyName>
</info>
</keyHolder>
</issuer>
</license>

The proposal enhances the join procedure. the node interaction protocol and the **content** storage procedure defined by Kademlia. In a preliminary initialization phase a node applies to the Certification Service for a certified NodeId and for bootstrap information outcoming messages: especially, the node must produce special credentials related to every **content** to be inserted in the DHT.

5.1.1 Initialization

Node A must obtain its own certified id, in order to interact with other peers...that establishes the expiration date of the signed (NodeId.sub.A). The CS keeps track of the association between UserId and AuthId, so that all **subsequent** NodeIdReq received by the same users receive in response the same AuthId passed earlier, unless it is expired or close to expiration. This is a...the first join using information obtained from the bootstrapList, each node should get in a different way a list of nodes to be contacted for **subsequent** join operations. For example a node can maintain its own list of trusted bootstrap nodes, or the same CS could periodically insert a signed bootstrapList...generated nonces. Messages sent at steps I and Ii must be somehow marked differently (e.g., different opcode). to distinguish the request from the response.

Authentication tokens are structured as follows:

(Auth.sub.AB) = Sign((NodeId.sub.B...against man in the middle attacks instead of exchanging timestamps because we cannot assume that hosts are synchronized to a common clock.

5.1.4 **Content** storage system

RPCs follow Kademlia's definitions, except for the store RPC. Let A be a node, owner of a **content** Obj. If A wants to store Obj in the DHT it locates via lookup the k nodes closest to the **content** key and then sends to them a store message structured as follows (suppose that B is a generic replica node):

A (right arrow) B : (AuthIdTTL, (K.sup.-.sub.A))

Cred binds the UserId to the key for which the **content** was inserted and to the hash code of the **content**, so that is subsequently possible to prove that the owner had inserted the **content** Obj at the key k. Cred includes also a timestamp and a time to live to specify the **content** submission time and its persistence period. During the periodic **content** spreading procedure, all replica nodes send store messages keeping the original credentials associated with each **content**. A node performing a lookup for contents related to a key (chi) receives all the objects marked with (chi) from replica nodes responsible for that key; before passing the **content** to the application, the node must verify the credentials signature and the object hash and must discard the object if the check fails.

If the application ascertain that the **content** is somehow polluted (e.g., the key that marks the **content** is not related with it), it can benefit from the information included in the credentials to penalize the owner of the **content**. This could be simply accomplished by instructing the underlying node to blacklist the cheater user in ...network, as well as integrated in the application, can help to exclude more rapidly the polluter from the whole network. Nevertheless, the propagation of polluted **content** is largely limited due to credentials' verification.

5.1. ...CS, the attacker cannot generate its id "ad hoc". Routing attacks (including eclipse) are unfeasible. Moreover, it is unfeasible for an attacker to hide a **content** marked with a given key k by way of a node insertion attack, because the malicious node cannot register a substantial number of nodes with...a set of references to invalid nodes (i.e., devoid of AuthIds), the victim node is not able to contact any of them because the **authentication** protocol fails in signature verification. If the attacker responds with a set of valid colluding nodes. its attack results ineffective because the colluders' ids are...this scheme. Nevertheless, each node corresponds to a different user account and the node initialization requires a verification procedure for that account. If the user **authentication** procedure requires a human interaction it would be difficult for an attacker to create many different nodes in an automated way, actually lowering the risk...CS when the submitted identity has been correctly authenticated.

Storage attacks Every storage entry in the DHT is bound with its Cred, created by the **content** owner with an unforgeable signature. A node performing a lookup operation returns to the application only those results that are bound with some Cred, and the consumed object depending on the quality of the **content**. The underlying node can be then instructed to exclude from network traffic those nodes whose reputation is too bad. The use of Cred can contrast attacks like index poisoning, **content** pollution or even DDoS attacks based on redirection by punishing the malicious users who attempt these attacks.

Man in the middle attack An attacker who...is limited to a node interaction session; moreover authenticators are addressee-specific, because they include the recipient node ID. Finally, the nonce based two-way **authentication** scheme grants protection against common interleaving attacks as Oracle session attacks, parallel attacks and offset attacks.

6 Prototype

In this Section we describe the main...3. in the implemented prototype the main application interacts with the user components described in Section 3. As already mentioned above, we assume that the **content** indexed and retrieved in the P2P network is always governed, requiting the adoption of an appropriate format which is able to provide a full description of the **content**. We used the MPEG-7 metadata for the multimedia **content** representation and MPEG-21 metadata to express the **digital rights**. Moreover we also consider protected contents, obtained by applying **encryption** tools for DRM. According to Chillout reference implementation (5), we make use of the DCI ...leave the system and to insert/retrieve the DCF files. As already described, it makes use of a DCI and DCF wrapper for parsing the **digital content** files and for extracting the metadata to be indexed.

The insertion of a **content** proceeds as follows: the **Content** Creator component is responsible for creating the DCI and the DCF. The user can choose one or more resources to be published in the P2P network in a single DCF file and can associate to each resource a different **license**, which can be completely customized for different purposes. It is worthwhile noticing that some resources in the DCF file could be also encrypted to ensure that even if they are retrieved from the P2P network the consumption of the **content** is possible only to the principal specified in the **license**. Once the DCF (or simply the DCI) is created, it can be shared on the structured peer-to-peer

network. Concerning the **content** retrieval, the lookup operation on the DHT could be done by simple keywords or structured bundle of MPEG-21 REL tags, resulting, at low level, in the index of the **content** whose DCF (DCI) is fulfilling the request. The Application module contacts then the publishing sources (peers) asking for more information about the **content**. Every user can check the **license** conditions associated to a given **content** before downloading it. The Transport component communicates by means of a DCFMetadataService on a separate channel (socket), with a specific protocol which is able to means of the CollectorResults, which generates a separate thread looking for the asynchronous return messages. The user can select the specific **content** from the result list and the Application component will contact the specific owner source (the <IP addressthrough the FileTransportation component (see Figure 3) which communicates We have described a decentralized, distributed and secure communication infrastructure for indexing and retrieving multimedia contents with associated **digital** tights. We have discussed a feasible approach to share **digital** items according to the associated **license**, making use of a P2P routing infrastructure based on DHT. Complex queries on standard MPEG-7 and MPEG-21 multimedia metadata are supported.

Concerning the in the MPEG consortium. MPQF lets us also investigate novel approaches for searching **digital** contents on peer-to-peer infrastructure, as range and by feature queries that could be introduced into a future prototype. Moreover, we plan to evaluate within the framework of the PRIN "PROFILES" project (7).

Received: August 31, 2008

References

(1) MPEG-7--ISO/IEC 15938--Information Technology Multimedia **Content** Description Interfaces. http://www.chiariglione.org/mpeg/ standards/mpeg-7/mpeg-7.htm. Last visited: 15 Nov 2008.

(2) MPEG-21--ISO/IEC 21000--Information Technology Multimedia Framework. http://www.chiariglione.org/mpeg/ standards/mpeg-21/mpeg-21.htm. Last visited: 15 Nov 2008.

(3) MPEG-21 **Rights** Expression Language--ISO/IEC 21000-5--Information Technology Multimedia Framework. http://www.chiariglione. org/mpeg/technologies/mp21-rel/ index.htm. Last visited: 15 Nov 2008.

(4) **Digital** Media ...Tous and Jaime Delgado. L7, An MPEG-7 Query Framework. In AXMEDIS '07: Proceedings of the 3rd International Conference on Automated Production of Cross Media **Content** for Multi-Channel Distribution, Barcelona, Spain, pages 256-263. IEEE Computer Society, 2007.

(29) Walter Allasia, Francesco Gallo, Filippo Chiariglione, and Fabrizio Falchi. An Innovative Approach for Indexing and Searching **Digital Rights**. In AXMEDIS '07: Proceedings of the 3rd International Conference on Automated Production of Cross Media **Content** for Multi-Channel Distribution, Barcelona, Spain, pages 147-154. IEEE Computer Society, 2007.

(30) CreativeCommons. http:// creativecommons.org. Last visited: 15 Nov 2008.

(31) MPEG-A-- ISO/IEC 23000-5--Information Technology Multimedia Application Format. Part 5: Media **Streaming** Application Format. http://www.chiariglione.org/mpeg/ standards/mpeg-a/mpeg-a.htm. Last visited: 15 Nov 2008.

(32) **Digital** Media Project (DMP). Approved Document No. 3--Technical Specification: Interoperable DRM Platform, Version 3.0--1003/GA15. http://www. dmpf.org/open/dmp1003.zip. Last visited: 15 Nov 2008.

(33) MPEG-21 **Rights** Expression Language--ISO/IEC 21000-5 Amendment 3 : the OAC (Open Access **Content**) profile.

(34) MPEG-21 **Rights** Expression Language--ISO/IEC 21000-5 Amendment 2: the DAC (Dissemination And Capture) profile.

(35) TV-Anytime. http://www.tv-anytime.org. Last visited: 15 Governed **content** distribution on dht based networks. internet and Web Applications and Services, 2008. ICIW '08. Third International Conference on. pages 391-396. June 2008.
(36) Marco...

View: HTML | PDF | Word

☐ Q3 2008 Wave Systems Corporation Earnings Conference Call - Final

Date: Nov 10, 2008

3/6,K/3 (Item 3 from file: 15)
04900384 1601022321
**

Q3 2008 Wave Systems Corporation Earnings Conference Call - Final

Nov 10, 2008
Word Count: 15656
Text:

...non-GAAP category, an important measure of our financial performance as we believe it best represents the continued increase in our demand for our software **license** upgrades. Consistent with our revenue recognition policies, this outline in the Company's 10-K, as software upgrade billings grow we would expect to see...
...were approximately 57,896,000 shares and 49,737,000 shares respectively. At September 30, 2008, Wave had total assets of $2,985,000 and **subsequent** to the close of the third quarter, Wave completed a $721,500 offering of Series J convertible preferred stock and began to implement a series...

...example, it works with the Boston subway token actually, the MyFare Card which is a contactless smart card could actually be enrolled as a contactless **authentication** token with your Dell E-Series platform.

So if you happen to traveled through Boston or you're in Boston, you can use one of...wanted a very high performance laptop wanted to be able to buy the highest performance drives. And now Seagate has made available with full disk **encryption** their highest performance drive products for notebooks.

So really there is now no reason to buy a laptop without a full disk encrypting drive. And...

...reporters who got that connect the dot there not really correct.

So we're very pleased to continuing to supply Dell with the full disk **encryption** software that ships natively from the factory. One of the huge advantages that Dell has in the marketplace today is that their PC's come...we are seeing continued connection with the enterprise's focus on moving towards hardware. Still a tremendous amount of this business is around the data **encryption** side, the encrypted drives.

Although we're seeing many more customers who are deploying the encrypted drives and also deploying some of the features and...

...been were light by a significant number.

And we have no reason to believe that that won't be fully made up for in the **subsequent** weeks that have already slipped. We saw some of that in the marketplace, as well, where there were new systems that were ordered, that subsequently...ad that talks about vPro, under vPro there is something called anti-theft technology and that encompasses both the

trusted platform module and a data **encryption** capability.

We demonstrated in August the data **encryption** capability with a technology that was originally code named Danbury, and is now called Anti-theft, and Danbury provides full disk **encryption**, but from the motherboard side of the PC.

This is important because this capability will show up in Intel chip sets on a worldwide basis across all platform vendors. So if those companies who want to take full advantage of the native data **encryption** capabilities of the Intel chip set. Wave has a solution that can provide that and provide seamless capability, same look and feel of software, same ...

...And we have also demonstrated support for Toshiba's new full disk encrypting drives as well. So as the industry branches out and moves data **encryption** into hardware, Wave intends to provide the software to support that underlying hardware in a very common set of screens, common set of capability, really...ve seen divisions of some of the big health insurance companies -- in general as I said before, they are purchasing because of the full disk **encryption** side.

There is a mixture, there is a mixture of companies that have never bought any data **encryption** before and this was just a logical way to step into data **encryption** and it was easy to buy and easy to implement. We've also had customers who we have worked with for the better part of nine or 12 month who have either got data **encryption** employed, or are in detailed researching it with other software vendors. In general, the best customers are the ones who have already had an experience with one of the top four or five software full disk **encryption** products.

And I don't need to pick on any one of their brands, the comments are equal across the board that the general enterprise...push in a pin number to complete the long distance call. In essence a password for every phone call you made.

In the transition to **digital** cell phones, they put a security chip in your phone that basically has the identity of your phone. And since then, the global cellular industry...the future is cloud computing and we're all going to be logging on to everything we do all the time, then what is the **authentication** token. What is the standard way that we secure our relationships to all of these services?

What we need is what feels like a set...small little business with two or three employees should have an encrypted drive in her PC. Or she is in violation of the Mass data **encryption** law, okay?

ROBERT EILER: Okay.

STEVEN SPRAGUE: So I keep looking at this and going -- now that has only been a law for four weeks...

...information, a social security number, a bank account number, you do not need any PIN numbers, just the person's bank account number. Driver's **license** or any other -- government ID card number.
Then you must have the data encrypted. So anyone who currently does state tax filings would be a...

...really should be sold with an encrypted drive.

And how long is it going to take everybody to get that message? So let's just **play** that a little bit larger, because that is a very simplistic example. I have to audit my service providers. So my lawyers, my

accountants. ADP...

.. data on your machines. can you provide me with a certificate that says it is encrypted? So being the fun, entertaining Company in the data **encryption** space we've tried this, and barely anybody knows what we're talking about.

ROBERT EILER: So --

STEVEN SPRAGUE: So there is an education. but...

...It in a state which is not secure. And so we're off following that path as well.

But I'm a pretty sophisticated data **encryption** person to go ask this set of questions. So it has been intriguing to watch the impact ... for the effect to roll across all the enterprises. big and small. So there is no question that the demand and need for full disk **encryption** is absolutely there. There is a regulatory requirement for it.

You're seeing it move into hardware. I think significant events, if your looking for a significant event over the course of the next period of time, look for other drive manufacturers adding **encryption**. So it's great that we have got Hitachi and Seagate and Toshiba. You want to see more. And I think as you continue to...couple of different kinds of questions I would like to ask you. What protects us from like a hostile takeover? It is our intellectual property **rights**?

STEVEN SPRAGUE: My 20,000 individual shareholders, what price will you take? And I mean this in the most polite way. Wave is a company...have so much broader reach than we do. So if you look at the Dell fliers going out right now. they talk about the data **encryption** in the drives. And we find that to be a much more effective path.

Today about 85% of all of our new customer contacts come...who watched our application watched five hours of video. To give you some context on that, a viewer who watched on the sort of generic **streaming** Microsoft platform watched one hour of video during the length of the Olympics.

It was an interesting event because it had a very finite number... ...event in any way. shape or form.

But I think we accomplished the purpose, which was we really demonstrated the viability of a download and **play** capability within the Microsoft Media Center. And I think it is clearly a direction that will add value to the media capabilities of the PC...

...today. We thank you for your participation and ask that you would disconnect your lines.

[Thomson Financial reserves the right to make changes to documents, **content**, or other information on this web site without obligation to notify any person of such changes.

In the conference calls upon which Event Transcripts are...

.. ADVISED TO REVIEW THE APPLICABLE COMPANY'S CONFERENCE CALL ITSELF AND THE APPLICABLE COMPANY'S SEC FILINGS BEFORE MAKING ANY INVESTMENT OR OTHER DECISIONS.]

View: HTML | PDF | Word

☐ Toward semantics-aware management of intellectual property **rights**

Date: 2007

3/6,K/4 (item 4 from file: 15)
03324736 1222483691
**

Toward semantics-aware management of intellectual property **rights**

2007
Word Count: 5083
Toward semantics-aware management of intellectual property **rights**

Abstract:

The purpose of this paper is to introduce the advantages of semantics-aware representation formalisms in the integration of **digital rights** management (DRM) infrastructures grounded on heterogeneous formats. After discussing the notion of semantics-aware IPR and its relationship with Semantic Web-style metadata, we exemplify...

Text:

Papers from the First European Workshop on Technological and Security Issues in **Digital Rights** Management (EuDiRights'06).
Mariemma Yague

lace=+Bold; Introductionface=-Bold;

The information and entertainment industry is one of the fastest growing and most profitable sectors of today's economy. Distributing information in **digital** form, however, raises numerous concerns due to the fact that it is difficult for **digital content** providers to control what others do with the information. This is especially true on the Internet, which is highly vulnerable to unauthorised use of information. Unauthorised distribution, forgery and defacement of **digital content** have become widespread, triggering a technological "arms race" between **content** providers and malicious users. For the last 10 years the industry has been demanding an efficient mechanism for **digital content** protection.

Digital Rights Management (DRM) technologies supporting secure transmission of **digital** products from publishers to consumers have become a crucial factor in the marketing of **digital content**. In general DRM systems seek to manage access to **digital content**, restricting it to individuals or organisations that are entitled by payment or affiliation to have access. **Digital content** managed by DRM can take many different forms, including music, information, software applications,

video and even enterprise e-mail. First generation DRM technologies focused on **encryption**-based solutions for locking **digital content** and limiting its distribution to authorised users. Early DRM techniques included limiting the number of devices on which **content** could be accessed or the number of times it could be accessed; imposing forward locks to prevent onward transmission of **content**, or withholding access until the user had registered with the **content** owner or publisher. **Digital** watermarking is also part of this palette of techniques, as it provides the basis for legal action if a violation of **rights** is detected.

While early DRM solutions addressed the issue of unauthorised copying, they did so at the expense of a substantial limitations to the publishers...

...even well known examples of particular solutions that have had rather unfortunate and unforeseen side effects, e.g. exposing user machines to security vulnerabilities.) Modern **content** delivery channels are more and more multi-tenanted, involving **content** owners, **content** aggregators, network owners, service providers, terminal manufacturers and DRM solutions providers. Also, increasing end user concerns about fair usage and privacy must be addressed.

Today, innovative second generation DRM solutions are needed, capable of flexibly supporting new opportunities to do business with **digital** information products. This increased flexibility is largely expected to be due to XML-based **Digital Rights** Management Languages (DRML) that declaratively assign usage **rights** to **digital content** ((21) Open **Digital Rights** Language, n.d.; (15) eXtensible right Mark-up Language, n.d.). DRMLs allow the description of specifications of **rights**, fees and usage conditions, together with message integrity and entity **authentication**. For instance, in the video-on-demand industry there is growing interest in switching from the usual download-to-display to a novel download-to...

... of video applications could be expressed as a DRML policy change. However, DRML's expressive power is bound by the metadata specifying properties of the **digital content** to which they refer.

In this paper we deal with associating DRMLs with advanced Semantic Web style metadata, highlighting the role of reasoning and inference... ...face=+Italic; (2003), some basic notions of DRM can be easily captured by basic entity-relationship modelling. Current DRM systems involve three main entities: Users, **Content** and **Rights**. Users create and use **digital content**, i.e. any type of **digital** product. **Rights** are privileges, constraints and obligations regarding **content**; they are granted or denied to users. DRM languages have been designed to state assertions about allowable permissions, constraints, obligations and any other **rights** -related relationship between users and **content**. **Rights** expressions can become very complex, and their correct enforcement needs a complete specification of the DRML semantics. Nonetheless, a full formalisation of DRM models is...

... 25) Sans and Cuppens, 2004) and David Bjorner ((2) Arimoto face=+Italic; et al.face=-Italic; , 2006). Referring to the original Gunter/Weeks/Wrights model, **rights** expressions consist of four parts:

face=+Italic: Permissionsface=-Italic; . What a right allows to do.

face=+Italic: **Rights** holdersface=-Italic; . Who is entitled to a right.

face=+Italic; Constraintsface=-Italic; . Any restriction on the right that may apply.

face=+Italic; Obligationsface=-Italic; . What...

...issues. DRM systems pose a series of well-known management problems:

- face=+Italic; Policy managementface=-Italic; . An entity should define and continuously enforce policies about **digital** products as part of its business strategy.

- face=+Italic; **Rights** management and licensingface=-Italic; . When **rights** are acquired from other entities, it is important to remember the source, how broad the **rights** are, etc. Also some business models require **rights** to be transferable, i.e. an entity can **license** some **rights** to other entities.

- face=+Italic; Revenue collectionface=-Italic; . ...traditional business models associate billing to right transfer (e.g., when buying a CD), while others generate revenue only when the user actually exercises the **rights**. Practical DRM systems must specify how to collect, account and share revenues.

Summarising, a DRM system is composed of a well-specified **rights** model/language (DRML) and of a set of advanced management tools. (Of course, legal aspects are also an important part of the picture, and may have an important impact on modelling issues. For the sake of conciseness, however, they are not discussed further in this paper.) **Rights** models and languages must be highly expressive in order to satisfy flexibility requirements posed by modern business models; also they must be as standardised as possible. In the next sections we introduce two XML-based DRMLs, XrML (eXtensible **rights** Mark-up Language) and ODRL (Open **Digital Rights** Language), and highlight their expressive power limitations.

face=+Bold; Limitations of XML-based DRMface=-Bold;

As we have seen, evolving business models for **digital content** introduced novel requirements for DRM systems. In this section we describe the motivations stimulating research on DRM policy languages (DRMLs) and their role toward interoperable enforcement of Intellectual Property **Rights** (IPR) on the Web. With respect to access control (AC) policy languages, DRMLs have many distinguishing features.

A first difference is multi-tenancy, i.e...

...number of actors involved in each transaction being regulated. Traditional AC typically involves two actors: a user requesting a resource, and a service provider requiring **authentication** in order to grant it. Third parties (e.g., certification authorities) may be involved but usually represent super-parties, entities that do not directly participate...

...service provider (e.g., the contract with an Internet provider or mobile communication company). By contrast a DRM transaction involves at least four actors: the **content** provider, the distributor delivering the **content**, the clearinghouse managing licences, and the end user buying licences. These actors cooperate along the **digital** media value chain according to the specific **rights** held by each party. Orchestrating this process is therefore more complicated than accessing a resource on a secure server.

Another crucial factor in DRM is...

.. motivate the need for a highly expressive DRML supporting a broad choice of radically different business models. The specific business model being implemented (pay-per-**play**, usage metering, download-to-own) dictates the strategies for regulating access to resources; furthermore, hardware and software solutions allow for tracking the actual usage of resources and enforce the **rights** associated with them.

For these reasons current XML-based DRMLs support fine-grained descriptions of resources, business processes and actors. Mainstream examples are ODRL (Open **Digital Rights** Language) and XrML (eXtensible right Mark-up Language), the latter forming the basis for MPEG-21 REL. More proposals are available, e.g. XMCL ((3...

...actual transactions, and the latter allows for a more cross-vertical applicability. Moreover, the specific environment in which DRM is applied (e.g., e-books, **streaming** media, mobile services) and the different hardware/software support by media players introduce specific requirements and functionalities.

In order to show the importance of interoperability between distinct DRMLs, Figure 1 (Figure omitted. See Article Image.) displays a possible scenario for policy re-use. In Workflow (a) the **content** provider delivers media objects to customers via the Internet according to the MPEG-21 multimedia framework ((6) Bormans and Hill, 2002), therefore relying on the XrML format for policy specification. As soon as the same **content** has to be delivered to mobile appliances, typically using the OMA open standard for DRM ((22) Open Mobile Alliance, 2003), it is necessary to translate...

...enforcement. Rewriting policies is a cumbersome task because media objects are supposed to be added continuously; also, this process can be automatic, such as in **content** aggregation, and consequently human supervision cannot always be considered in the translation process. Instead, in Workflow (b) a translation tool takes care of converting XrML ...some examples of semantics-aware DRM approaches. The most straightforward use of semantics-aware metadata is providing a fine-grained description of resources being managed. **Digital** Asset Management (DAM) tools are typically used by **content** providers (e.g., authors) to describe and associate IP **rights** with their products. Even if DAM is traditionally kept separated from DRM, data produced by DAM tools comply with a fundamental DRM requirement, namely the ...

...of resources, e.g. DOI ((18) The International DOI Foundation, n.d.), Handle System ((9) Corporation for National Research Initiatives, n.d.). Advanced descriptions of **digital** products and of the associated **rights** can drive the brokerage of media products whenever distributors make them publicly available, overlaying their own **rights** on the existing IP **rights** and enforcing them via the DRM infrastructure. Consequently, it makes sense to consider **rights** (and formats associated with them) as dynamic properties spanning the whole **digital** product lifecycle.

This is the approach followed by the Adobe eXtensible Metadata Platform (XMP) ((1) Adobe, n.d.), which exemplifies the applicability of Semantic Web ..
...n.d.) assertions, which are used for binding the wide range of Adobe applications (Illustrator, Premiere, Acrobat, etc.) to a common workflow-integrating asset and **content** management, search facilities, and control mechanisms on possible secondary uses (e.g. DVD duplication). Metadata is stored as XMP packets that label resources; within them...

.. developed Regulatory Ontologieface=+Italic; sface=-Italic: for expressing IPR, formalised ODRL semantics using OWL ontologies, and also applying Semantic Web techniques to the MPEG-21 **Rights** Data Dictionary (RDD) {{12} Delgado face=+Italic; et al.face=-Italic; , 2004}. Also, Delgado pinpointed the need for interoperable workflow descriptions and proposed the OWL...our example we concentrate on this part of a KB and apply OWL DL semantics to integrate the ODRL permission model with the taxonomy of **rights** provided by XrML. Specifically, XML elements associated with these entities constitute concepts (or classes) in the TBox. On the other hand, assertions constitute the intensional...

...second case the same translation is applied to the XrML right model, and the resulting ontology is integrated with the one defined for ORDL. Equivalent **rights** in both categorisations can now be equalised and policies can be transparently applied to principals whose permissions are defined in either format. Figure 4 (Figure... ... right is totally ineffective (i.e. the user can obtain the same effect as a duplication operation). Moreover, a "move" operation implies the duplication and **subsequent** deletion of an asset. Both these **rights** should then be granted to principals in order for them to perform this operation.

Considering now the re-use subtree, it is obvious that the...relationships between "render" and "transport" operations, can fit into a simple tree representation. As in the previous case, it is possible to integrate the XrML **rights** model with an ontology-based infrastructure. More interestingly, XrML and ODRL policies can be made interoperable with each other by mapping the two ontologies introduced in this paper. As an example, the homonymous "**play**" and "print" operations from both formats can be made equivalent. As a consequence, principals with a "display" permission in the ODRL expression language can be given the " **play**" and "print" **rights** on resources being protected by XrML metadata. Figure 7 (Figure omitted. See Article Image.) displays the sample mapping of ODRL permissions with XrML **rights**.

face=+Bold; Conclusionsface=-Bold;

Digital Rights Management languages allow asserted **rights** over **digital content** to be expressed in a machine-readable format. Today, DRM policies are increasingly used in conjunction with more general metadata - for example, harvested from cataloguing systems. It is generally recognised that **rights** assertions of today's XML-based policy languages do not fully benefit from the highly expressive metadata of Semantic Web style descriptions. As a contribution...

...pdfs/whitepaper.pdf.

2. Arimoto, Y., Bjorner, D., Chen, X. and Xiang, J. (2006), "Alternative models of Gunter/Weeks/Wright's: models and languages for **digital rights**", JAIST/DEDR document.

3. Ayars, J. (2002), "The eXtensible Media Commerce Language (XMCL)", available at: www.xmcl.org/specification.html.

4. Baader, F., Calvanese, D...

.. mpeg/standards/mpeg-21/mpeg-21.htm.

7. Chong, C., Corin, R., Etalle, S., Hartel, P., Jonker, W. and Law, Y. (2003b), "LicenseScript: A novel **digital rights** language and its semantics", , IEEE Computer Society Press, New York, NY, pp. 122-9, available at:

http://citeseer.ist.psu.edu/chong03licensescript.html.
8. Chong, C., Etalle, S. and Hartel, P.H. (2003a), "Comparing logic-based and XML-based **rights** expression languages", Lecture Notes in Computer Science, Vol. 2869, pp. 779-92.

9. Corporation for National Research Initiatives (n.d.), "The handle system", available at...

...Samarati, P. (2006b), "Modality Conflicts in semantics-aware access control",

12. Delgado, J., Gallego, I. and Garcia, R. (2004), "Use of semantic tools for a **digital rights** dictionary", EC-Web, pp. 338-47.

13. Delgado, J., Gallego, I., Llorente, S. and Garcia, R. (2003), "Regulatory ontologies: an intellectual property **rights** approach", OTM Workshops, pp. 621-34.

14. DL Implementation Group (n.d.), Available at: http://dl.kr.org/dig/.

15. eXtensible right Markup Language (XrML...

...XrML) 2.0", available at: www.xrml.org.

16. Gunter, C.A., Weeks, S.T. and Wright, A.K. (2001), "Models and languages for digitals **rights**", .

17. Haarslev, V. and Moler, R. (2001), "Description of the racer system and its applications", , pp. 131-41.

...International DOI Foundation (n.d.), "The DOI system", available at: www.doi.org/.

19. Llorente, S., Rodriguez, E. and Delgado, J. (2004), "Workflow description of **digital rights** management systems", OTM Workshops, pp. 581-92.

20. Mindswap (2004), "SWOOP - a hypermedia-based featherweight OWL ontology editor", available at: www.mindswap.org/2004/SWOOP/.

21. Open **Digital Rights** Language (n.d.), "ODRL 1.1", available at: http://odrl.net/1.1/ODRL-11.pdf.

22. Open Mobile Alliance (2003), "OMA **digital rights** management", available at: at: www.openmobilealliance.org/docs/DRM%20Short%20Paper%20DEC%202003%20.pdf.

23. Parsia, B., Sirvin, E., Grove, M. and Alford, R...
...formalisation des langages de DRM", Inforsid.

26. Tous, R., Garcia, R., Rodriguez, E. and Delgado, J. (2005), "Architecture of a semantic XPath processor, application to **digital rights** management", EC-Web, pp. 1-10.

27. Yague, M.I., Mana, A., Lopez, J., Pimentel, E. and Troya, J.M. (2003), "A secure solution for commercial **digital** libraries". Online Information Review, Vol. 27 No. 3, pp. 147-59.

28. W3C (n.d.), "Resource Description Framework (RDF)", available at: www.w3.org/RDF...

.. use

Figure 4: The categorisation of ODRL permissions

Figure 5. The OWL ontology derived from the ODRL permission model

Figure 6: The categorisation of XrML **rights**

Figure 7: Integration of ODRL permissions and XrML **rights^**

View: HTML | PDF | Word

☐ Charting your course: follow the silicon-bread-crumb trail in this directory to find the perfect device for your project.

Date: August 04, 2005

3/6,K/5 (Item 5 from file: 9)
03751093 Supplier Number: 135245681
Charting your course: follow the silicon-bread-crumb trail in this directory to find the perfect device for your project.

August 04, 2005
Word Count: 8797

TEXT:

...devices to support applications ranging from high-volume-consumer to high-performance, high-reliability products. Actel will deliver the "soft" ARM7 family core with a **license**-free business model. Designers can use the Core8051 8-bit microcontroller core in Actel's nonvolatile, single-chip FPGAs, including ProASIC3, ProASIC Plus, Axcelerator, SX...

...and workstations, and it extends the x86 ISA (instruction-set architecture) across 32- and 64-bit PC, server, and workstation platforms with the AMD64 technology. **Subsequent** enhancements of the AMD Athlon and AMD Opteron processor lines extend 64-bit x86 computing to the embedded-system market. The ElanSC5220 x86 controller covers...

...AMD added the Alchemy Au1200 processor to the AMD Alchemy line to better target low-power, high-performance PMP (personal-media-player), automotive, and DMA (**digital**-media-adapter) applications.

* ALTERA

Altera continues to improve its integrated-product portfolio. HardCopy II uses a fine-grained collection of Hcell transistors. It builds on...

...introduced the network-enabled ADSP-BF534, BF536, and BF537 processors, as well as the BF566-eM30 eMedia Platform, which targets IP set-top boxes, triple-**play** devices, portable and networked media players, and automotive-safety/driver-assistance systems.
The ADuC702x precision analog-microcontroller family combines on a single chip embedded precision analog functions and **digital** programming. Featuring ARM7-based programmability, the ADuC702x is the newest addition to the company's MicroConverter series-a portfolio of 8052-based devices. MicroConverter products target high-precision measurement and control and data-acquisition systems with basic **digital**-programming needs. The precision analog microcontrollers

integrate a 32-bit RISC core and flash memory with precision data-conversion technology that supports as many as 16 channels of fast, 12-bit-accurate analog-to-**digital** conversion and as many as four 12-bit DACs.

' APPLIED MICRO CIRCUITS CORP

Since acquiring a portfolio of products associated with IBM's 400 PowerPC ...

...Octeon devices include hardware acceleration essential for Level 3 to Level 7 applications, which includes packet processing, TCP, multicore scaling, compression/decompression, pattern matching, and **encryption**.

The Nitrox Soho Secure Communication Processor family targets wired and wireless broadband gateway for the SOHO (small-office/home-office), and SME markets, with performance...

...LOGIC

Cirrus Logic's EP93xx ARM9-based embedded processors target applications such as point-of-sale terminals, medical instrumentation, security and surveillance, process monitoring, and **digital** entertainment. These processors include WinCE. NET board-support packages and Linux kernel ports with Cirrus Logic's ARM third-party program support.

MaverickKey technology, which is standard on all Cirrus ARM9-based embedded processors except the EP9301, comprises the MaverickKey **digital-rights**-management tool and the MaverickCrunch advanced, mixed-mode, math coprocessor. MaverickKey technology allows designers to assign hardware IDs to protect against design piracy as products...

...control functions in consumer, industrial, office-automation, telecom, and automotive applications. PSOC devices integrate an 8-bit processor core with programmable blocks of analog and **digital** logic in eight-to 100-pin devices in DIP, SSOP SOIC, MLF, and TQFP packages. All PSOC devices are dynamically reconfigurable during runt/me, enabling...

...consumer electronics, HIDs (human-interface devices), and home and industrial automation. The CY8C21x23 and CY8C21x34 families are Cypress' smallest and least costly PSOCs with four **digital** and four analog configurable peripheral blocks. The general-purpose CY8C21x34 microcontroller supports capacitive touch-sense applications with no external components. These PSOC families target consumer... in-system-programmable flash memory ranging to 64 kbytes. The secure microcontrollers target applications demanding protective measures against IP (intellectual-property) theft. These devices employ **encryption** techniques that support ATMs, point-of-sale terminals, and data-logging applications.

The network microcontrollers provide low-cost connections for networking applications and include a...

...devices use a microcontroller core running at 75 MHz with an extended 22-bit addressing range. The mixed-signal microcontrollers feature 12-bit analog-to-**digital** conversion and dual 8-bit PWM channels that are combinable to 16 bits, as well as multiple serial ports and extended parallel I/O.

* EM. .

...enabled household appliances. These 32-bit microcontrollers incorporate networking-security features, onboard ROM and RAM, and support for IPv6.

The MB9140x supports IPv6 and includes **encryption** circuitry supporting the AES (Advanced Data **Encryption** Standard), DES (Data **Encryption** Standard), and 3DES (Triple DES). The **encryption** circuits are 150 to 200 times faster than software-based **encryption** and are complemented by **authentication** circuitry. The series also supports the MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm 1) **authentication** standards, key exchange methods DH 1/DH 2, and the IKE (Internet Key Exchange) protocol with a hardware engine.

The newest members of Fujitsu's...

...conditioning, data-acquisition, processing, and control applications. Features for these devices include a hardware multiply-accumulate unit, an ADC, an op amp, a current source, **digital** potentiometers, and communication interfaces. The Versa microcontroller series of low-cost, 8-bit, 8051 -based microcontrollers are cost-efficient drop-in replacements for industry-standard...

...wireless-access points), VPN (virtual-private-network) equipment, and more.

IDT's RC32434 Interprise integrated communications processor, operating as fast as 400 MHz, targets the **digital** home network, which includes multimedia applications, such as media servers, media adapters, and IP (Internet-Protocol)-based network appliances. The integrated nonvolatile RAM and an **authentication** unit for security functions enable **digital-content**-protection applications and identification storage.

The RC32365 Interprise processor integrates a hardware-accelerated IPsec (IP-security) engine that improves the operating frequency by 20%, to...

...an extended family of network and communications processors targeting applications with increasing processing demands created by faster line speeds and deeper packet-inspection requirements of **content** -based services, as well as to support multiple protocols and evolving industry standards. The IXP460 and IXP465 network processors, the latest additions to the IXP4XX...

...a six-pin, SOT-23 package. The company integrated two low-pin-count PIC microcontrollers with the Keeloq cryptographic peripheral targeting secure-data-transmission and **authentication** applications, such as battery-clone elimination. The PIC16F785 makes it easier for power-supply designers to use the programmability of **digital** control in power-conversion applications by integrating analog building blocks.

Microchip brought many high-memory/ high-pin-count, 8-bit PIC18F microcontrollers to production, including...

...an SPI serial interface (rather than PCI or ISA). Microchip also offers a free TCP/IP stack for all PIC18s.

The dsPIC family of DSCs (**digital**-signal controllers) features a DSP engine with 30-MIPS nonpipelined performance implemented with a C-compiler-friendly microcontroller architecture and design environment. The 20 dsPIC30FXXXX...

...new software libraries for the dsPIC, many free or available for a one-time fee.

* MIPS TECHNOLOGIES

MIPS Technologies offers processor architectures and cores targeting **digital** consumer and business applications. The company licenses its 32- and 64-bit RISC IP (intellectual property) to semiconductor companies, ASIC developers, and system OEMs. Core...

...electronics and other embedded-system applications. The 64-bit VR Series MIPS-based microprocessors provide high-performance and scalability targeting embedded systems from Internet and **digital** consumer devices to servers and switches.
Over the past year, NEC expanded its 32- and 8-bit microcontroller offerings. The company introduced to the V850 family the V850E2/ME3, a 32-bit microcontroller for use in inverters, industrial equipment, printers, and **digital** consumer products. On the 8-bit side, NEC announced the 78K0/Fx series of microcontrollers for automotive-body applications and the 8-bit 78K0/Kx2...

...QuickMIPS family combines an embedded-processor subsystem and programmable logic on a single die. QuickLogic develops intellectual property and software to target applications that distribute **digital** media over Internet Protocol networks, including in-car infotainment, **digital** signage, overhead projectors, and medical imaging. QuickLogic offers modules, such as video compression/decompression, **encryption**
, and **digital**
-
rights
management. This device architecture provides opportunities for designers to make trade-offs in implementing system functions in hardware for improved performance or in software for...

...The M16C and M32 families target consumer applications, and Renesas' AE series chips smart-card platforms have 68 kbytes of EEPROM and a 1024-bit **encryption** coprocessor.

Renesas introduced three new groups of devices in the low-pin-count, small-package R8C/Tiny series that suit cost-sensitive applications; these 16...

...control applications.

* SILICON STORAGE TECHNOLOGY

Silicon Storage designs and manufactures various densities of flash-memory components, flash mass-storage products, and flash microcontrollers targeting the **digital**-consumer, networking, wireless-communications, and Internet-computing markets. SST's flashFlex51 family of 8-bit, Superflash CMOS microcontroller products implements the 8051 architecture and instruction...

...security features. The flash-Flex51 microcontrollers target the high-reliability, high-flexibility, low-voltage, and low-power requirements of today's computer peripherals, communication equipment, **digital** consumer/appliances, and networking applications.

* STMICROELECTRONICS

STMicroelectronics offers 8-, 16-, and 32-bit microcontrollers and microprocessors, including a family of ARM7-based microcontrollers, and application...
...platform of ultra-low-power, 16-bit RISC microcontrollers targets battery-powered measurement applications and enables systems to simultaneously interface to analog signals, sensors, and **digital** components. The architecture features power consumption at 0.1 mA for RAM retention, 0.8 mA during real-time-clock mode, and 250 mA/MIPS...

.. density embedded memory with ultralow power consumption. Toshiba launched the TX4939XBG-400, its first embedded PCI-based processor using 90-nm process technology; it targets **digital**-consumer applications. Toshiba also introduced the TX9956CXBG; operating at 533 or 666 MHz, it targets multifunction printers and high-end set-top-box applications.

Continuing...

...execute on its strategy to offer focused platforms, Toshiba introduced the AVM49R TX System RISC multimedia reference platform for IP (Internet Protocol) set-top box, **digital**-multimedia appliances, and home gateways.

* TRANSMETA

Transmeta develops and offers computing technologies that improve performance, reduce power consumption and control heat generation in electronic devices...

...word) engine that can execute as many as eight instructions per clock cycle; a 1-Mbyte L2 cache; and support for MMX (multimedia extension), SSE (**streaming**-single-instruction-multiple-data-extension), SSE2, and SSE3 instructions.

* UBICOM

Ubicom offers wireless-network processors that can implement communication and control functions in software, so...

...turbo mode.

* VIA TECHNOLOGIES

Via offers power-efficient processors for the x86 personal-electronics and embedded-device markets with a range of feature-rich Via **digital** -media chip sets. Via divides its processors into five product families that it bases on power consumption and performance criteria ranging from fanless operation to...

View: HTML | PDF | Word

☐ Charting your course: follow the silicon-bread-crumb trail in this directory to find the perfect device for your project.(THE 32ND ANNUAL MICROPROCESSOR DIRECTORY)(Cover Story)

Date: August 4 , 2005

3/6,K/6 (Item 6 from file: 148)
0018625528 **Supplier Number:** 135245681 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Charting your course: follow the silicon-bread-crumb trail in this directory to find the perfect device for your project.(THE 32ND ANNUAL MICROPROCESSOR DIRECTORY)(Cover Story)

August 4 , 2005
Word Count: 10538 **Line Count:** 00913

.. devices to support applications ranging from high-volume-consumer to high-performance, high-reliability products. Actel will deliver the "soft" ARM7 family core with a **license**-free business model.

Designers can use the Core8051 8-bit microcontroller core in Actel's nonvolatile, single-chip FPGAs, including ProASIC3, ProASIC Plus, Axcelerator, SX...

...and workstations, and it extends the x86 ISA (instruction-set architecture) across 32- and 64-bit PC, server, and workstation platforms

with the AMD64 technology. **Subsequent** enhancements of the AMD Athlon and AMD Opteron processor lines extend 64-bit x86 computing to the embedded-system market. The ElanSC5220 x86 controller covers...

.. AMD added the Alchemy Au1200 processor to the AMD Alchemy line to better target low-power, high-performance PMP (personal-media-player), automotive, and DMA (**digital**-media-adapter) applications.

* ALTERA

Altera continues to improve its integrated-product portfolio. HardCopy II uses a fine-grained collection of Hcell transistors. It builds on...

...Introduced the network-enabled ADSP-BF534, BF536, and BF537 processors, as well as the BF566-eM30 eMedia Platform, which targets IP set-top boxes, triple-**play** devices, portable and networked media players, and automotive-safety/driver-assistance systems.

The ADuC702x precision analog-microcontroller family combines on a single chip embedded precision analog functions and **digital** programming. Featuring ARM7-based programmability, the ADuC702x is the newest addition to the company's MicroConverter series-a portfolio of 8052-based devices. MicroConverter products target high-precision measurement and control and data-acquisition systems with basic **digital**-programming needs. The precision analog microcontrollers integrate a 32-bit RISC core and flash memory with precision data-conversion technology that supports as many as 16 channels of fast, 12-bit-accurate analog-to-**digital** conversion and as many as four 12-bit DACs.

* APPLIED MICRO CIRCUITS CORP

Since acquiring a portfolio of products associated with IBM's 400 PowerPC...

...Octeon devices include hardware acceleration essential for Level 3 to Level 7 applications, which includes packet processing, TCP, multicore scaling, compression/decompression, pattern matching, and **encryption**.

The Nitrox Soho Secure Communication Processor family targets wired and wireless broadband gateway for the SOHO (small-office/home-office), and SME markets, with performance...

...LOGIC

Cirrus Logic's EP93xx ARM9-based embedded processors target applications such as point-of-sale terminals, medical instrumentation, security and surveillance, process monitoring, and **digital** entertainment. These processors include WinCE. NET board-support packages and Linux kernel ports with Cirrus Logic's ARM third-party program support.

MaverickKey technology, which is standard on all Cirrus ARM9-based embedded processors except the EP9301, comprises the MaverickKey **digital-rights**-management tool and the MaverickCrunch advanced, mixed-mode, math coprocessor. MaverickKey technology allows designers to assign hardware IDs to protect against design piracy as products...

...control functions in consumer, industrial, office-automation, telecom, and automotive applications. PSOC devices integrate an 8-bit processor core with programmable blocks of analog and **digital** logic in eight-to 100-pin devices in DIP, SSOP SOIC, MLF, and TQFP packages. All PSOC devices are dynamically reconfigurable during runi/me, enabling...

...consumer electronics, HIDs (human-interface devices), and home and industrial automation. The CY8C21x23 and CY8C21x34 families are Cypress' smallest and least costly PSOCs with four **digital** and four analog configurable peripheral blocks. The general-purpose CY8C21x34 microcontroller supports capacitive touch-sense applications with no external components. These PSOC families target consumer... in-system-programmable flash memory ranging to 64 kbytes. The secure

microcontrollers target applications demanding protective measures against IP (intellectual-property) theft. These devices employ **encryption** techniques that support ATMs, point-of-sale terminals, and data-logging applications.

The network microcontrollers provide low-cost connections for networking applications and include a...

...devices use a microcontroller core running at 75 MHz with an extended 22-bit addressing range. The mixed-signal microcontrollers feature 12-bit analog-to-**digital** conversion and dual 8-bit PWM channels that are combinable to 16 bits, as well as multiple serial ports and extended parallel I/O.

' EM...

... enabled household appliances. These 32-bit microcontrollers incorporate networking-security features, onboard ROM and RAM, and support for IPv6. The MB9140x supports IPv6 and includes **encryption** circuitry supporting the AES (Advanced Data **Encryption** Standard), DES (Data **Encryption** Standard), and 3DES (Triple DES). The **encryption** circuits are 150 to 200 times faster than software-based **encryption** and are complemented by **authentication** circuitry. The series also supports the MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm 1) **authentication** standards, key exchange methods DH 1/DH 2, and the IKE (Internet Key Exchange) protocol with a hardware engine.

The newest members of Fujitsu's...

...conditioning, data-acquisition, processing, and control applications. Features for these devices include a hardware multiply-accumulate unit, an ADC, an op amp, a current source, **digital** potentiometers, and communication interfaces. The Versa microcontroller series of low-cost, 8-bit, 8051 -based microcontrollers are cost-efficient drop-in replacements for industry-standard...

...wireless-access points), VPN (virtual-private-network) equipment, and more.

IDT's RC32434 Interprise integrated communications processor, operating as fast as 400 MHz, targets the **digital** home network, which includes multimedia applications, such as media servers, media adapters, and IP (Internet-Protocol)-based network appliances. The integrated nonvolatile RAM and an **authentication** unit for security functions enable **digital-content**-protection applications and identification storage.

The RC32365 Interprise processor integrates a hardware-accelerated IPsec (IP-security) engine that improves the operating frequency by 20%, to ...

...an extended family of network and communications processors targeting applications with increasing processing demands created by faster line speeds and deeper packet-inspection requirements of **content** -based services, as well as to support multiple protocols and evolving industry standards. The IXP460 and IXP465 network processors, the latest additions to the IXP4XX...

... a six-pin, SOT-23 package. The company integrated two low-pin-count PIC microcontrollers with the Keeloq cryptographic peripheral targeting secure-data-transmission and **authentication** applications, such as battery-clone elimination. The PIC16F785 makes it easier for power-supply designers to use the programmability of **digital** control in power-conversion applications by integrating analog building blocks.

Microchip brought many high-memory/ high-pin-count, 8-bit PIC18F microcontrollers to production, including...

...an SPI serial interface (rather than PCI or ISA). Microchip also offers

a free TCP/IP stack for all PIC18s.

The dsPIC family of DSCs (**digital**-signal controllers) features a DSP engine with 30-MIPS nonpipelined performance implemented with a C-compiler-friendly microcontroller architecture and design environment. The 20 dsPIC30FXXXX...
...new software libraries for the dsPIC, many free or available for a one-time fee.

* MIPS TECHNOLOGIES

MIPS Technologies offers processor architectures and cores targeting **digital** consumer and business applications. The company licenses its 32- and 64-bit RISC IP (intellectual property) to semiconductor companies, ASIC developers, and system OEMs. Core...

...electronics and other embedded-system applications. The 64-bit VR Series MIPS-based microprocessors provide high-performance and scalability targeting embedded systems from Internet and **digital** consumer devices to servers and switches.

Over the past year, NEC expanded its 32- and 8-bit microcontroller offerings. The company introduced to the V850 family the V850E2/ME3, a 32-bit microcontroller for use in inverters, industrial equipment, printers, and **digital** consumer products. On the 8-bit side, NEC announced the 78K0/Fx series of microcontrollers for automotive-body applications and the 8-bit 78K0/Kx2...QuickMIPS family combines an embedded-processor subsystem and programmable logic on a single die. QuickLogic develops intellectual property and software to target applications that distribute **digital** media over Internet Protocol networks, including in-car infotainment, **digital** signage, overhead projectors, and medical imaging. QuickLogic offers modules, such as video compression/decompression, **encryption**, and **digital-rights** management. This device architecture provides opportunities for designers to make trade-offs in implementing system functions in hardware for improved performance or in software for...

...The M16C and M32 families target consumer applications, and Renesas' AE series chips smart-card platforms have 68 kbytes of EEPROM and a 1024-bit **encryption** coprocessor.

Renesas introduced three new groups of devices in the low-pin-count, small-package R8C/Tiny series that suit cost-sensitive applications; these 16...

...control applications.

* SILICON STORAGE TECHNOLOGY

Silicon Storage designs and manufactures various densities of flash-memory components, flash mass-storage products, and flash microcontrollers targeting the **digital**-consumer, networking, wireless-communications, and Internet-computing markets. SST's flashFlex51 family of 8-bit, Superflash CMOS microcontroller products implements the 8051 architecture and instruction...

...security features. The flash-Flex51 microcontrollers target the high-reliability, high-flexibility, low-voltage, and low-power requirements of today's computer peripherals, communication equipment, **digital** consumer/appliances, and networking applications.

* STMICROELECTRONICS

STMicroelectronics offers 8-, 16-, and 32-bit microcontrollers and microprocessors, including a family of ARM7-based microcontrollers, and application...

...platform of ultra-low-power, 16-bit RISC microcontrollers targets battery-powered measurement applications and enables systems to simultaneously interface to analog signals, sensors, and **digital** components. The architecture features power consumption at 0.1 mA for RAM retention, 0.8 mA during real-time-clock mode, and 250 mA/MIPS...

...density embedded memory with ultralow power consumption. Toshiba launched the TX4939XBG-400, its first embedded PCI-based processor using 90-nm process technology; it targets **digital**-consumer applications. Toshiba also introduced the TX9956CXBG; operating at 533 or 666 MHz, it targets multifunction printers and high-end set-top-box applications.

Continuing...

...execute on its strategy to offer focused platforms, Toshiba introduced the AVM49R TX System RISC multimedia reference platform for IP (Internet Protocol) set-top box, **digital**-multimedia appliances, and home gateways.

* TRANSMETA

Transmeta develops and offers computing technologies that improve performance, reduce power consumption and control heat generation in electronic devices...

...word) engine that can execute as many as eight instructions per clock cycle; a 1-Mbyte L2 cache; and support for MMX (multimedia extension), SSE (**streaming**-single-instruction-multiple-data-extension), SSE2, and SSE3 instructions.

* UBICOM

Ubicom offers wireless-network processors that can implement communication and control functions in software, so...

...turbo mode.

* VIA TECHNOLOGIES

Via offers power-efficient processors for the x86 personal-electronics and embedded-device markets with a range of feature-rich Via **digital**-media chip sets. Via divides its processors into five product families that it bases on power consumption and performance criteria ranging from fanless operation to...

View: HTML | PDF | Word

☐ Media security thwarts temptation, permits prosecution.(Industry Trend or Event)

Date: June 22 , 2000

3/6,K/7 (Item 7 from file: 148)
12414842 **Supplier Number:** 63691442 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Media security thwarts temptation, permits prosecution.(Industry Trend or Event)

June 22 , 2000
Word Count: 8362 **Line Count:** 00707

Text:

RAMPANT PIRACY OF UNPROTECTED **DIGITAL** MEDIA HAS **CONTENT** DEVELOPERS AND DISTRIBUTORS SCRAMBLING TO CONSTRAIN, REDEFINE, AND EXPLOIT THIS "NEW WORLD ORDER." IN DEVELOPING YOUR MEDIA-RECORDING AND -PLAYBACK DEVICES, BEWARE OF CREEPING SECURITY...

NUMEROUS LAWSUITS, some of which have already returned verdicts against the defendants, attempt to curtail the illegal distribution of copyright-protected **digital** media, such as electronic books, still images, audio files, and video movies. Rock band Metallica and rap artist Dr Dre have even taken the unusual step of pursuing legal action not only against a software company whose product supposedly promotes such **content**-sharing, but also against several universities whose students swap files using the school-supplied computer networks. Consortiums such as the Recording Industry Association of America...

...purchase a significant percentage of audio CDs and videotapes, have enjoyed speedy broadband Internet access for years, thanks to their university accounts. With ADSL (asymmetrical-**digital**-subscriber-line) and cable modems now entering homes in a big way, even more traditional music and video consumers can quickly download and stream multimegabyte files.

Where are these files coming from? Today's high-powered PCs can achieve bit-accurate extraction of CD audio **content** and compress it to one-twelfth (MP3) or even one-twenty-fourth (MS Audio) its original size with little-to-no discernible quality loss (Reference 1). Both extraction and compression occur several times faster than ordinary playback speeds, and **digital** copies retain much higher quality than bootlegs made in the analog past. Multigigabyte hard drives are now pervasive, as are fast-writing CD-recordable drives...

...onto a CD. Large-screen, high-resolution computer monitors can easily display high-definition images, portable MP3 and MiniDisc players are obsoleting analog tape, and **digital** speakers and high-definition-TV displays are establishing footholds in homes.

In attempting to stem the flood of illegal media sharing, the **content** creators and distributors and you, their equipment-manufacturer partners, must walk a thin line. On the one hand, you're enforcing the valid copyright claims of those who developed the material. However, you can't excessively constrain customers who are exercising their legal **rights** to make copies for their own use of media they own and to transfer ownership of that purchased media to others. Media-security, or DRM (**digital-rights**, management) systems should be invisible to honest users (this invisibilty is called "eliminating false positives"), while acting as strong deterrents to pirates. And, to simplify...

...attempting to standardize a means of coping with this diversity of options via the Commission's OPIMA (Open Platform Initiative for Multimedia Access).

Ideally, the **content** should be decoupled from its access **rights**, so that if a consumer upgrades or replaces equipment, to which the access **rights** frequently link, he or she need not obsolete an existing media-library collection. If the security system benefits only the **content** creators and distributors, consumers' lukewarm response shouldn't be surprising. If, however, security safeguards pacify **content** developers' concerns and therefore enable consumers to access a broader and richer set of media than they've been able to enjoy in the past...

...high-fidelity, multichannel surround sound; smaller files for a given quality level; and otherwise-unavailable clips, such as concerts, music videos, and interviews.

Ultimately, the **content** developers are free to put whatever restrictions they choose on their media. They can prohibit decoded audio from passing over a **digital** connection to speakers or **digital**-video streams from passing to a monitor. They can restrict the playback rate over these **digital** channels to prevent high-speed duplication. They can embed "watermarks"--copyright and usage-**rights** information--that obstruct playback or otherwise restrict usage with noncompliant systems (see sidebar "Back to basics"). They can even attempt to retrofit media to prohibit...

...usage, the more complicated the systems become, increasing the potential for end users' frustration. And, because compliance with industry consortiums such as the (SDMI) Secure **Digital** Music Initiative is voluntary, not mandatory, the first major **content** developer or distributor that loosens its restrictions in response to predicted or actual consumer confusion, lowers the bar for everyone.

ONLY AS STRONG AS ITS WEAKEST LINK

Figure 1 shows one possible **digital**-media-distribution system of today for technologically savvy users or of the near future for everyone else. The first point of **digital**-media downloading will probably be a PC using a cable modem or an ADSL connection. However, it could also be a cable, terrestrial or satellite **digital** set-top box, a media server, an Internet- enabled **digital** audio or video player, or even an advanced cellular phone or personal **digital** assistant.

{Figure 1 ILLUSTRATION OMITTED}

Once consumers access a copy of the **content**, they might want to stream, copy, or move it to other media peripherals in their home or office. A variety of distribution mechanisms is possible, including Ethernet cable, IEEE 1394, and USB 2.0, home-phone-line networking, power-line-network connections, or even wireless. And, to **play** the file, why bother with the multiple analog-to-**digital** and **digital**-to-analog conversions, resolution limitations, and noise coupling, all of which degrade quality, of traditional audio and video cable? Instead, your customers will probably want to run a pure-**digital** connection to their speakers over S/PDIF (Sony/Philips **Digital** Interface) or USB and to a display over a DVI (**Digital** Visual Interface). At no point in this process, however, can unprotected **digital** data be "in the clear" (also called "plaintext") so that people can copy it.

Regarding downloading versus **streaming**, the **content** distributors would probably prefer to transmit only a temporary, quickly discarded bit stream to each customer. Imagine, for example, paying a monthly subscription fee to...

...song from any album in that label's catalog 24 hours a day, seven days a week. This scenario maintains maximum distributor control over the **content**, but it doesn't let a user listen to the music on a non-Internet-tethered device. Consumers are also familiar and comfortable with going to record stores and purchasing tapes and CDs; the e-commerce analogy is a **digital** music file. So, a DMX (**Digital** Music Express)-like distribution system for music will probably supplement but not replace downloading and archiving, though **streaming** within the home, such as from a PC to an audio receiver via a Turtle Beach AudioTron or an equivalent, is feasible.

Streaming-only delivery of video material is a more likely scenario, replicating today's pay-per-view and cable-channel subscriptions and partially driven by the...

...undoubtedly be willing to pay an additional fee for archiving capability. In general, you should anticipate some resistance if you provide no ability to record **digital** broadcasts, given that analog-broadcast archiving is possible. And, just as individuals rent or even buy DVDs and video tapes so that they can start, pause, and finish viewing the **content** at their leisure, there'll most likely be a demand for similar capabilities in the **digital** age. **Digital**-video-capture capability at degraded quality levels is one possible compromise.

In differentiating between **streaming** and downloading-and-playing usage models, it's also important to distinguish between the ability to view material and the ability to capture or copy it. This distinction is key to resolving the misconception regarding the infamous DeCSS (**content**-scrambling system) utility, which circumvented the **encryption** for DVDs. Duplication of DVD media has always been technically possible, though the high cost of writable DVDs and drives currently makes it economically unfeasible. DeCSS simply lets you view DVD **content** as well as defeat region coding. It's also important to note that the developers of DeCSS didn't break the CSS algorithm itself. In...

...less common than cracking an implementation of that algorithm," says

Mark Ashida, president and CEO of media-security-software company and Intel spin-off PassEdge.

Streaming media, in light of its impermanent nature, can tolerate a less robust **encryption** scheme than downloading-and-playing media, which is fortunate because the near-immediate-response expectations of **streaming** viewers don't allow for complex **encryption** and decryption calculations. However, the **encryption** must be distributed throughout the media, not just in the file header, so that illegal tapping into the bit stream partway through the broadcast is impossible. Typically, you want to reauthorize the connection using a new key pattern every fraction of a second to few seconds. Any evaluation of **encryption**-algorithm alternatives must also consider that the low cost expectations of consumer-electronics equipment are at odds with the high processing power, memory, and gate...

...also encompasses renewability: the ability to detect and block access by a compromised platform, such as a player attempting to use a key that the **content** developer has voided.

Lack of renewability is a key limitation of many of today's security systems, such as the smart-card-based techniques that...

...software programs that can disable Macrovision or otherwise restore the original video signal. Also, secure delivery of media to customers is only half the task. **Content** distributors would like ...patterns, both for planning future products and for targeting consumers for advertising on related products. You need to balance these suppliers' desires with your customers' **rights** to privacy. Not everyone would like others to know what types of books they read, pictures or movies they look at, or music they listen...

...server of its own, distributing further media variants.

To better understand this concept, consider the SDMI scheme (Figure 2). SDMI requires that any device storing **digital** audio contain a 32-bit predefined manufacturer ID or 128-bit random number to generate security keys. Where does this identifier come from? One possible...

... over to your friend's house to listen to them.) However, this approach has downsides, too. If the media is lost or irreparably damaged, the **rights** to the media disappear. Media portability also raises the specter of illegal duplication, a scenario that can only be detected if, for example, two people...

...sensing and amplifying thermal noise patterns across undriven resistors, and a secure communication channel links the firmware hub to the I/O hub.

From an **encryption** standpoint, SDMI doesn't care which of a multitude of possible **encryption** and decryption and compression algorithms you choose. As Matt Perry, vice president and general manager of the Embedded Processor Division at Cirrus Logic, describes it, the **encryption** portion of the SMDI protocol is only a functional specification and, therefore, is open to numerous **encryption** and audio-codec implementations. However, DMI's Version 1.0 specification defines a specific watermark technique that Verance developed and DVD Audio also plans to...

...access levels. SDMI 1.0-compliant devices must search for the Verance watermark at least every 15 seconds. SDMI-compliant hardware will carry the DMAT (**Digital** Music Access Technology) stamp of approval.

The not-yet-finalized SDMI 2.0 specification defines another set of watermarks. They include a "do-not-import...

...compliant "ripping" (extracting-to-hard-drive) program (Reference 3). SDMI 1.0-compliant players must search for the 2.0-indicating"trigger" and then cannot **play** SDMI-compliant media until the user upgrades

the player firmware. These additional proposed watermarks may inhibit users' abilities to **play** their MP3 libraries. If implemented in the final specification, these additional security measures will likely trigger a consumer uproar like the one that the "millennium...

...If the media that stores the files can interrogate the player and block playback if it detects the presence of a compromised unit, additional access **rights** become available. This concept is central to the definition of the SD (Secure **Digital**) card, defined by the so-called 3C (three-company) Entity: Matsushita, Sandisk, and Toshiba. SD cards contain a protected media-key block describing all valid...

...should also keep media-key-block information up to date in the SD-card manufacturing line.

(Figure 3 ILLUSTRATION OMITTED)

SD cards incorporate the CPRM (**Content** Protection for Recordable Media) Protocol, which, along with the CPPM (**Content** Production for Prerecorded Media) Protocol, the 4C (four-company) Entity--IBM, Intel, Matsushita, and Toshiba--developed. CPRM and CPPM derive from the same CSS **encryption** scheme that the 4C Entity developed for DVD video and DVD audio disks. DVD Video's circumvented security, which DeCSS exemplifies, has compelled DVD-audio advocates to delay mass production until they can come up with a more robust alternative **encryption** approach. However, the revocation capability of CPRM has enabled SD deployment to proceed.

Current **encryption** technologies as well as those now under development promise to enable high-speed and easy interchange of **digital** media within homes and offices. Standards bodies have yet to endorse an official approach for IEEE 1394, but the emerging de facto standard appears to be the **Digital** Transmission Copy Protection algorithm that the 5C (five-company) Entity--Hitachi, Intel, Matsushita, Sony, and Toshiba--developed. **Encryption** over TCP/IP (Transmission Control Protocol/ Internet Protocol) has existed in numerous forms for some time and applies to traditional Ethernet as well as to HomePNA (Home Phone Networking Alliance) and HomePlug Powerline Appliance network connections. **Encryption**, **authentication**, and frequency-hopping are integral to the Bluetooth, HomeRF, and IEEE 802.11 specifications. Both powerline and wireless networking techniques must comprehend sufficient safeguards to ensure that your neighbors can't illegally access the media. You can also apply the DTCP (**Digital** Transmission **Content** Protection) Protocol for IEEE 1394 to USB.

SHUFFLING THE BITS

What if your customer wants to connect a set of **digital** -interface speakers to his or her audio playback device or hook up a video-playback unit to a **digital** flat-panel display or CRT? These links also must be secure. Most of today's **digital** speakers employ S/PDIF connections, whose limited SCMS (Serial Copy Management System) **encryption** hasn't stood up to the test of time. Until **encryption** support becomes pervasive in USB-equipped devices, **content** developers will have muted enthusiasm for the concept of audio-playback systems with "live" **digital** outputs.

IEEE 1394 currently provides insufficient bandwidth to enable the transmission of uncompressed high-resolution video streams. For this purpose, you must turn to the...

...transition-minimized differential signaling). DVI's secure variant, which Intel announced and Silicon Image demonstrated in February at its Developer Forum, is HDCP (High-bandwidth **Digital** Copy Protection) (Figure 4). Silicon Image is currently shipping samples of first-generation HDCP-aware DVI Sil 168 transmitter and Sil 861 receiver chips and slates production of both for the third quarter of 2000.

(Figure 4 ILLUSTRATION OMITTED)

Like SDMI for audio, HDCP supports the concepts of **authentication** to verify that a display device is licensed to

receive protected **content**, **encryption** of the transmitted video to prevent "eavesdropping" on the protected **content**, and renewability to enable the revocation of compromised devices. HDCP's hybrid-block/stream-cipher approach encrypts data at the transmission end of each 1.65-Gbps channel and decrypts it at the other side. The approach uses the more robust block cipher during **authentication**. Both the authorized host and display device have access to a set of secret keys that the HDCP **license** administrator supplies. The secret keys consist of an array of 40 56-bit secret device keys and a corresponding 40-bit binary key-selection vector (KSV). The host initiates **authentication** by sending an initiation message containing its KSV and a 64-bit value. The display device responds by sending a response message containing its KSV...

...can calculate a shared value, which, if both devices have a valid set of keys, is equal. The devices use this shared value in the **encryption** and decryption of the protected **content**. **Authentication** has now been established, and reauthentication occurs every 2 sec, or each time the connection is lost for any reason. A faster, bitwise-exclusive-OR-based stream cipher handles **content** delivery. If the HDCP **license** administrator discovers that the security of a certain display device has been compromised and the secret device keys are exposed, the administrator places the KSV...

...list when it receives a valid, newer SRM than that currently held in memory. SRMs can be presented to the host in prerecorded or broadcast **content**, or received from another compliant device with a newer SRM. **Encryption** and decryption logic add approximately 10,000 logic gates to the transmitter- and receiver-chip designs.

UNDER THE HOOD

So much for media that passes between systems. What about security within a system? The degree of vulnerability caused by an "in-the-clear" **digital** bit stream passing between chips inside a system depends on how "open" the system is. A proprietary, nonupgradable set-top box, for example, realistically isn...

...most hard-core hackers, who would think nothing of tapping into a board trace or probing a packaged IC's leads to siphon off a **digital** bit stream.

On the opposite end of the spectrum, however, consider PCs. A number of available third-party software packages disable Macrovision protection for DVD movies, enabling dubbing to video recorders through a graphics card's video output. High Criteria's Total Recorder software intercepts a **digital**-audio bit stream on the way to the PC's sound card. Streambox VCR performs a similar function for video. And the sound cards in some PCs digitally output any audio bit stream routed to them and ignore SCMS copy-protection bits at their **digital** inputs.

The emergence of **digital**-TV receivers and decoder hardware and software for PCs exposes another potential source of duplication. In an approach such as the one that Ravisent Technologies advocates with its CinePlayer DTV, a low-cost add-in card handles the **digital**-TV reception and demodulation tasks and then sends the combined audio, data, and video bit stream across the PCI bus to software running on the...same device, never revealing the system-specific key. The Micronas device even integrates the D/A converter, so that neither the decrypted nor the decoded **digital**-audio information is ever exposed.

Future operating-system enhancements, placing system-specific **encryption** at their core instead of as add-ons, will also help boost security while maintaining platform openness. Microsoft spent a lot of time at April...

...any user concerned with privacy can disable any identification scheme the company comes up with, even though such a step might prohibit access to certain **content**. Third-party hardware and software developers

will also need to add security hooks to their drivers so that they won't lose access if a certain media type insists on operating only with secure programs.

AT A GLANCE

* Burgeoning **digital** text, audio, and video media combine with high-speed Internet access, high-performance computers, and cheaper and denser storage to create a piracy potential that...

...nightmares.

* When evaluating security algorithms for incorporation within your systems, be sure to balance robustness with ease of use and performance.

* Don't let the **content** developers' and distributors' fear and greed lead you to implement features that circumvent privacy or restrictions that violate consumers' duplication and transfer **rights** for their legally obtained media.

* An ideal security system combines the concepts of **authentication**, **encryption**, and renewability.

BACK TO BASICS

People often use the terms "**encryption**" and "watermarking" interchangeably. In truth, the terms refer to different technologies, although both are important aspects of a comprehensive **digital**-**rights**-management system, and you can sometimes use watermarking to implement **encryption**.

Two main types of **encryption** exist. Symmetrical, or synchronous, **encryption** uses the same security key to "lock" and scramble an outgoing file and to recover a bit-exact copy of the original **content** at the destination. Examples of symmetrical **encryption** include the now-broken DES (Data **Encryption** Standard); its interim replacement, triple-DES, which, as the name implies, runs each data packet through DES **encryption** three times; next-generation AES (Advanced **Encryption** Standard); and RC (Rivest's Cipher). The primary advantage of symmetrical **encryption** is its high-speed encoding and decoding, which occurs because the algorithms employ relatively simple transposition and substitution steps. The Achilles' heel of the approach...

...third party. If something intercepts the bit stream and the unintended recipient figures out the key, the media is vulnerable. On the other hand, clever **encryption** can result in the delivery of a legitimate-appearing but incorrect piece of media, such as a bogus memo, to a recipient using an invalid key.

Asymmetric, or asynchronous, **encryption** employs dual keys (Figure A). The sender encrypts the media with the recipient's public key, and the recipient decrypts it with his or her private key. Exchange of public keys requires no secure channel, and the recipient can ensure **authentication** of a valid sender. However, the key-generation, **encryption**, and decryption algorithms, commonly based on prime-number techniques, require multiplication operations that are time-consuming and performance-intensive. Asymmetric **encryption** examples include the RSA (Rivest, Shamir, and Adelman) and Diffie-Helman algorithms.

(Figure A ILLUSTRATION OMITTED)

Hybrid schemes that combine asymmetric and symmetric **encryption**, such as a combination of RSA and DES, are also possible. Consider, for example, the approach that HDCP (High-bandwidth **Digital** Copy Protection) takes. Asymmetric **encryption** establishes the initial authorization between host and display, as well as the periodic reauthorization. Faster symmetric compression handles the **content** transfer. Any performance-critical application can incorporate a similar approach. DTCP (**Digital** Transmission Copy Protection) comprehends support for both asymmetric and symmetric protocols. It supports symmetric protocols for their supposed lower value, single-and free-copy material.

Streaming delivery is the key target of RPK SecureMedia, a

New Zealand (therefore not subject to US export restrictions) cryptography company funded by, among others, **streaming**-media pioneer RealNetworks. RPK claims that its proprietary approach combines the benefits of public/private-key systems, such as **authentication**, **digital** signatures, certificates, and key management, with the speed of symmetric systems in one **encryption** and decryption engine. The Encryptonite Tookit offers a choice of 80 levels of security using 127- to 2281-bit-long keys. Detractors point to the fact that no one knows how robust RPK's proprietary **encryption** algorithms are, because they haven't been subjected to the same intense scrutiny as standards-based alternatives, such as those from Intel spin-off PassEdge... that, aside from greater initial latency analogous to a FIFO-buffer fill, increased key length does not degrade performance. The company is developing hardware-based **encryption** and decryption accelerators to supplement its software offerings.

PassEdge's StreamAccess **encryption** algorithms take advantage of any hardware-accelerated integer arithmetic logic within a microprocessor, such as Intel's MMX (multimedia-extensions) instruction set. The company targeted...

...may have been when you held a piece of paper up to a strong light and saw a faint, normally invisible, manufacturer or publisher logo. **Digital** "fingerprinting" applies the same concept to electronic media. Watermarking might find use as a means of hiding the secure key in symmetrical **encryption**. More commonly, however, **content** distributors use watermarking to encode copyright and other media source information, and to document usage regulations. These rules include duration of access, the number of times a user can access the media under certain purchase conditions, duplication capability (or lack thereof), and geography-based access **rights** (such as a movie that you can **play** in the United States but not in Europe). Internet search "spiders" can then use all of this embedded data to detect illegal media distribution and...

...application-defined greater file size or bit rate), it also must tolerate transmission errors; a watermark can't be voided by dropped packets during a **streaming** transmission or circumvented by selective deletion of portions of a picture or sound clip.

Digimarc is perhaps the best-known image-watermarking company. Photo steganography...

...frame-by-frame watermarking would probably be overkill as well as too time-consuming and expensive.

One common technique available to those wishing to watermark **digital** audio involves injection of low-level broadband and time-independent noise. As with still images, you need to balance transparency--the inability to hear the...

...the technology behind the MPEG audio (most notably MP3) and newer AAC (advanced audio codec) algorithms, has also spent much time and effort on audio **encryption** and watermarking. The company's watermarking approach is high-performance, which is important when companies must generate **license**-specific versions of media. The approach also can operate on already-compressed audio files (references B and C). It either slightly increases the bit rate to hold quality constant or partially decodes, then more aggressively quantizes and adds watermarking bits to, perceptually irrelevant frequency bands.

Fraunhofer's **encryption** technique is equally interesting (references D and E). The company encrypts each group of audio samples within the encoding processes of spectral decomposition, temporal and frequency masking, and quantization and then descrambles before inverse quantization and filter-bank resynthesis (Figure B). Embedding **encryption** within encoding allows the **encryption** algorithm to selectively place its manipulations in certain frequency

bands. This flexibility means that you can create an encrypted file that an audio decoder without access to the proper key can still **play**, albeit with an adjustable amount of distortion. Applying this concept to e-commerce means that a customer could preview entire songs versus today's short clips and then purchase a key to enable access to them at their full quality.

(Figure 8 ILLUSTRATION OMITTED)

For more information on **encryption**, check out references F and G. Good Web sites to continue your ...REFERENCES

(A.) Jajodia, Sushil, and Neil F Johnson. "Exploring steganography: seeing the unseen," IEEE Computer, February 1998, pg 26.

(B.) Herre, Jurgen, and Christian Neubauer, "**Digital** watermarking and its influence on audio quality," 105th Audio Engineering Society Convention, Sept 26 to 29, 1998, San Francisco, CA.

(C.) Herre, Jurgen, and Christian...

...Herre "Secure delivery of compressed audio by compatible bit-stream scrambling," 108th Audio Engineering Society Convention, Feb 19 to 22, 2000, Paris.

(F.) Cravotta, Nicholas, "**Encryption**: more than just complex algorithms," EDN, March 18, 1999, pg 105.

(G.) Schneier, Bruce, Applied Cryptography: Protocols, Algorithms and Source Code in C, Second Edition, ISBN # 0471117099, John Wiley & Sons, 1995.

BELATEDLY CLOSING PANDORA'S BOX

As Hollywood and the consumer-electronics companies drag their feet in finalizing the Secure **Digital** Music Initiative specification, they ironically exacerbate the copyright-infringement problem by continuing to churn out audio CDs without any security whatsoever and DVD videos with already-compromised illegal-access safeguards. Efforts under way by a number of vendors strive to retrofit **digital** media with **encryption** and watermarking capabilities, but legal restrictions and potential hardware and software incompatibilities limit their success.

The Copyright Act of 1976 allows consumers to make as...

...not allowed, except in academic settings.) The act's 1992 amendment (commonly known as the Audio Home Recording Act) somewhat restricted this consumer freedom for **digital**-audio media, prohibiting **subsequent** duplication of first-generation **digital** copies in conjunction with the Serial Copy Management System (SCMS).

Production of any system that circumvents SCMS is illegal, but so too is any approach that doesn't allow consumers to make first-generation copies of their legally obtained **digital** music. Some of the copy-restricting products now under development, although perhaps acceptable outside the United States, come close to violating or blatantly violate consumer **rights** under the Home Audio Recording Act. And this discussion concerns only audio. The Macrovision copy protection embedded within the analog output of DVD video players, as well as encoded in some video-cassettes and videodisks, reflects the fact that even analog duplication of video **content** is illegal. The 1998 **Digital** Millennium Copyright Act, whose legality the US Supreme Court has yet to determine, goes one step further in outlawing attempts to circumvent any copyright-protection...

...audio CDs on computer CD-ROM drives. According to the manufacturers, dedicated audio-CD players, because of their greater tolerance of media errors, can still **play** altered audio CDs (Reference A). However, consumer feedback suggests that reality falls short of this goal. Both systems can optionally disable a CD player's **digital** output, an infringement of consumer **rights** under the Home Audio Recording Act and of the Red Book CD standard. Undeterred, TTR Technologies, whose MusicGuard technology also blocks duplication of audio **content** on CDs, is working on extending its technology to DVDs.

Divx may be dead, but companies are still trying to figure out how to

render...

...leading restricted-playback proponents, claims to have figured out how to ensure that, once a consumer opens any optical media's packaging, the disk will **play** only for a **content** -distributor-specified period of time. A touted environmentally friendly chemical that the company applies to the disk is the secret, and the last step in...

...Unlike Divx, Spectra Science's approach requires neither an expensive, custom DVD player, nor that the player connect via phone line to a server for **authentication** and, some feared, Big Brother snooping of consumer viewing habits.

REFERENCES

(A.) Starrett, Robert A. "Recording at the speed of sound," eMedia, May 2000, pg 28.

SECURING--AND CIRCUMVENTING--AT HIGH SPEED

A key part of the reason that your chosen **encryption** system should be upgradable, aside from the potential for cracking due to inadvertent disclosure of keys, is the ever-increasing performance of stand-alone and...with the high performance of a hard-wired ASIC, and the logic block structures are ideal for implementing the types of arithmetic functions common in **encryption** and decryption. At FPGA 2000, representatives from the Worcester Polytechnic Institute (Worcester, MA) used Xilinx XCV1000s to implement the Serpent block cipher (one of the Advanced **Encryption** Standard candidates) at **encryption** rates beyond 4 Gbps (Reference B). The researchers evaluated four design approaches with varying gate counts and speeds.

The 2.44- to 37.97-MHz...

...Computing Machines (FCCM 2000) (Reference C). Using the company's XCV150 FPGAs with Java-based dynamic partial-reconfiguration techniques, Xilinx engineers achieved 10.7-Gbps **encryption** performance using the DES (Data **Encryption** Standard) algorithm.

REFERENCES

(A.) Kim, Hea Joung, and William H Mangione-Smith, "Factoring large numbers with programmable hardware," ACM/SIGDA International Symposium on Field Programmable...

...Serpent block cipher," ACM/SIGDA International Symposium on Field Programmable Gate Arrays, Feb 10 to 11, 2000, Monterey, CA.

(C.) Patterson, Cameron, "High performance DES **encryption** in Virtex FPGAs using JBits," IEEE Symposium on Field-Programmable Custom Computing Machines, April 17 to 19, 2000, Napa, CA.

FOR MORE INFORMATION ...

For more...

...9416

www.1394ta.org

Enter No. 345

4C Entity

www.4centity.com

Enter No. 346

Bluetooth Special Interest Group

www.bluetooth.com

Enter No. 347

Digital Display Working Group (DVI)

www.ddwg.org

Enter No. 348

Digital Transmission Copy Protection Licensing Administrator (5C Entity)
www.dtcp.com
Enter No. 349

Electronic Frontier Foundation
1-415-436-9333
www.eff.com
Enter No. 350

Home Phoneline Networking Alliance
www.homepna.org
Enter No. 351

HomePlug Powerline Alliance
www.homeplug.org
Enter No. 352

Home Recording **Rights** Coalition
1-800-282-8273
www.iec.ch/opima
Enter No. 353

HomeRF Working Group
1-503-291-2563
www.homerf.org
Enter No. 354...

...212-327-4044
www.mpa.org
Enter No. 357

Recording Industry Association of America
1-202-775-0101
www.riaa.org
Enter No. 358

Secure **Digital** Association
1-831-623-2107
www.sdcard.org
Enter No. 359

Secure **Digital** Music Initiative
1-858-826-2655
www.sdmi.org
Enter No. 360

USB Implementers Forum
1-503-296-9892
www.usb.org
Enter No. 361...of the airwaves; new technologies for audio copy protection," eMedia, September 1999, pg 50.

{5.) DeCarmo, Linden, "Safety in numbers; a look at the Secure **Digital** Music Initiative," eMedia, November, 1999, pg 48.

{6.) Lawton, George, "Intellectual property protection opens path for e-commerce," IEEE Computer, February 2000, pg 14.

(7.) Bell, Alan E. "The dynamic **digital** disk," IEEE Spectrum, October 1999, pg 28.
(8.) Caloyannides, Michael A. "**Encryption** wars: early battles," IEEE Spectrum, April, 2000, pg 37.
(9.) Drummond, Mike. "The Madison project," Stereo Review's Sound & Vision, November 1999, pg 119.
(10...

Product/Industry Names: 7372691 (Data **Encryption** Software)
Event Codes/Names:

View: HTML | PDF | Word

Records: 1 to 7 of 7